PULSIA

Política de Seguridad

CLASIFICACIÓN: GENERAL

PULSIA TECHNOLOGY

REGISTRO DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA
1	Edición Inicial	Octubre 2022
2	Actualización	Septiembre 2023
3	Actualización de Aprobación	Noviembre 2025

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

ÍNDICE

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

1. POLÍTICA DE SEGURIDAD

Las políticas de seguridad son un **conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa**. Se trata de un plan realizado para combatir los riesgos a los que está expuesta la empresa en el mundo digital. Tiene por objeto identificar responsabilidades y establecer principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por la empresa mediante las tecnologías de la información y de las comunicaciones, así como la estructuración de la correspondiente documentación de seguridad.

Detallan una serie de procesos internos de la empresa que se deben realizar de forma periódica para no mantenerlos vulnerables. Las políticas de seguridad **no solo van destinadas a los equipos técnicos e informáticos de una empresa, sino que van dirigidos a todos los puestos de trabajo que sean susceptibles de producir algún error o descuido de seguridad**. Cabe destacar que muchos de los problemas de seguridad de las empresas se producen por errores de las personas que no tienen en cuenta la vulnerabilidad de los datos y la información de la empresa.

1.1. Introducción

En este documento se expone la Política de Seguridad de la Información de PULSIA, como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete en el marco del Esquema Nacional de Seguridad. Asimismo, se detallan las precauciones y medidas de seguridad adoptadas para asegurar el correcto cumplimiento de la legislación vigente:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- ENS. Artículo 12. Organización e implantación del proceso de seguridad.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
- Ley 34/2002, de 11 de julio, de Servicios de la Información de Comercio electrónico, LSSICE.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

- Guía de Seguridad de las TIC CCN-STIC 805 ENS. Política de seguridad de la información.
- Guía de Seguridad de las TIC CCN-STIC 801 ENS. Responsabilidades y funciones.
- El convenio colectivo aplicable, correspondiente a “Empresas de consultoría, y estudios de mercado y de la opinión pública”.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- UNE-EN-ISO 9001, UNE-ISO-IEC_27001,

Normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a PULSIA.

Debemos tener en cuenta que la información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la empresa. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

La Seguridad de la Información es la protección de este activo cuya finalidad es la de asegurar la calidad de la información y la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio.

Asimismo, la seguridad de la información es un proceso que requiere de medios técnicos y humanos y una adecuada gestión y definición de los procedimientos y, en el que es fundamental la máxima colaboración e implicación de todo el personal de la empresa.

La dirección de la empresa, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento.

1.2. Definiciones

- **SISTEMA DE INFORMACIÓN**: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- **RIESGO**: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- **GESTIÓN DE RIESGOS**: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
- **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)**: sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

- **DISPONIBILIDAD**: Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.
- **INTEGRIDAD**: La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- **CONFIDENCIALIDAD**: La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- **AUTENTICIDAD**: Se debe asegurar la identidad u origen de la información.
    - Trazabilidad: Se debe asegurar para ciertos datos quién hizo qué y en qué momento.

2. OBJETIVOS Y FUNDAMENTOS DE ESTA POLÍTICA

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción. Por ello, se establecen los siguientes principios mínimos:

- **PRINCIPIO DE CONFIDENCIALIDAD:** los sistemas de información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.
- **PRINCIPIO DE INTEGRIDAD Y CALIDAD**: se deberá garantizar el mantenimiento de la calidad de la información, así como de los procesos de tratamiento de estableciéndose los mecanismos para asegurar que los procesos de creación, almacenamiento y distribución de la información contribuyen a preservar su corrección.
- **PRINCIPIO DE DISPONIBILIDAD Y CONTINUIDAD**: se garantizará un nivel de disponibilidad en los sistemas de información y se dotarán los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.
- **PRINCIPIO DE GESTIÓN DE RIESGO**: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

- **PRINCIPIO DE PROPORCIONALIDAD EN COSTE**: la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegurará que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.
- **PRINCIPIO DE CONCIENCIACIÓN Y FORMACIÓN**: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.
- **PRINCIPIO DE PREVENCIÓN**: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.
- **PRINCIPIO DE DETECCIÓN Y RESPUESTA**: los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia respondiendo eficazmente, a través de los mecanismos establecidos al efecto, a los incidentes de seguridad.
- **PRINCIPIO DE MEJORA CONTINUA**: se revisará el grado de cumplimiento de los objetivos de mejora de la seguridad planificados anualmente y el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la Administración Pública.
- **PRINCIPIO DE SEGURIDAD TIC EN EL CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN**: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- **PRINCIPIO DE FUNCIÓN DIFERENCIADA**: la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.
- **La Política de Seguridad de la Información** es aprobada por la Dirección de la empresa y su contenido y el de las normas y procedimientos que la desarrollan es de obligado cumplimiento.
- Todos los usuarios con acceso a la información tratada, gestionada o propiedad de la empresa tienen la obligación y el deber de custodiarla y protegerla.
- **La Política y las Normas de Seguridad** de la Información se adaptarán a la evolución de los sistemas y de la tecnología y a los cambios organizativos y se alinearán con la legislación vigente y con los estándares y mejores prácticas de la norma del Esquema Nacional de Seguridad.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

- **Las medidas de seguridad y los controles físicos**, administrativos y técnicos aplicables se detallarán en el Documento de Aplicabilidad y la empresa deberá establecer una planificación para su implantación y gestión.
- **Las medidas de seguridad y los controles** establecidos serán proporcionales a la criticidad de la información a proteger y a su clasificación.
- **Los usuarios** que incumplan la Política de Seguridad de la Información o las normas y procedimientos complementarios podrán ser sancionados de acuerdo con lo establecido en los contratos que amparen su relación con la empresa y con la legislación vigente y aplicable.

3. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

PULSIA establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- **ALCANCE ESTRATÉGICO**: La seguridad de la información deberá contar con el compromiso y apoyo de la Dirección de PULSIA, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.
- **ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD**: La seguridad de la información compromete a todos los miembros de la organización. PULSIA identifica los responsables y establece sus responsabilidades al efecto en el apartado de “Roles, responsabilidades y deberes” de este documento. La Política de seguridad y la normativa serán conocidas por todos los miembros de la organización.
- **GESTIÓN DE PERSONAL**: Todo el personal de PULSIA relacionado con la información y los sistemas es formado e informado de sus deberes y obligaciones en materia de seguridad, esencialmente mediante los procedimientos de seguridad que en cada caso procedan y mediante la normativa de uso de los activos. Sus actuaciones son supervisadas según los roles establecidos para verificar que se siguen los procedimientos definidos.

  Los accesos de los usuarios son únicos y se verifican de forma periódica sus derechos y las actividades que tienen que ver con la Seguridad de la información para corregir o exigir responsabilidades en su caso.
- **PROFESIONALIDAD, CONCIENCIACIÓN Y FORMACIÓN**: La seguridad de los sistemas es gestionada y revisada por personal de PULSIA cualificado y personal

externo especializado, que recibe y actualiza la formación necesaria para garantizar la seguridad de la información.

La presente Política de Seguridad de la Información debe ser conocida por todos los usuarios internos y externos y por las empresas que accedan, gestionen o traten datos de la empresa.

El conjunto de Políticas, normas y procedimientos complementarios a esta Política de Seguridad de la Información también deberán ser adecuadamente comunicados y puestos en conocimiento de las personas, empresas e instituciones afectadas o implicadas en cada caso.

Se definirán, periódicamente, programas de comunicación, concienciación y formación y se entregará copia de la normativa correspondiente a los usuarios.

- **AUTORIZACIÓN Y CONTROL DE LOS ACCESOS**: El acceso a los sistemas de información es controlado, monitorizado y limitado a los usuarios, procesos, dispositivos y sistemas de información con las mínimas funcionalidades permitidas y/o autorizadas.
- **SEGURIDAD INTEGRAL**: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.
- **PROTECCIÓN FÍSICA DE LAS INSTALACIONES**: La infraestructura que aloja los sistemas de la organización se encuentra ubicada en las instalaciones del proveedor de hosting contratado, las cuales deben contar con medidas de seguridad física, mecanismos de control de acceso, sistemas de redundancia, continuidad de negocio y condiciones ambientales adecuadas.
- **GESTIÓN DE RIESGOS**: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.
- **CONTRATACIÓN Y ADQUISICIONES**: Todas las contrataciones y adquisiciones que supongan o requieran acceso o tratamiento de información clasificada como no pública, deberán realizarse amparadas por un contrato que incluya cláusulas destinadas a garantizar la salvaguarda de la confidencialidad, integridad y disponibilidad de información.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

En aquellos casos en los que los servicios contratados supongan acceso o tratamiento por el proveedor de datos de carácter personal se deberá incluir en el contrato el clausulado requerido para el cumplimiento de la LOPDGDD y sus desarrollos.

Las empresas y personas que con motivo de contrataciones de servicios o adquisiciones de cualquier tipo accedan a información confidencial o de uso interno, deberán conocer la Política de Seguridad de la Información y las normas y procedimientos complementarios que sean de aplicación para el objeto de la contratación.

Las empresas y personas externas que accedan a la información de la empresa deberán considerar dicha información, por defecto, como confidencial. La única información que podrán considerar como no confidencial es aquella que se haya obtenido a través de los medios de difusión pública.

- **INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA**: En PULSIA los sistemas se evalúan de manera periódica para conocer en todo momento su estado de seguridad, tomando en consideración las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que procedan, y gestionando de esta manera la integridad de los mismos.

  Todos los elementos de los sistemas requieren autorización previa a su instalación.

- **PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO**: La información se clasifica de acuerdo con la sensibilidad requerida en su tratamiento y según los niveles de seguridad y protección exigibles.

  PULSIA presta especial atención a la información almacenada o en tránsito a través de entornos inseguros. Esto incluye a la información almacenada o tratada en equipos portátiles, tabletas, smartphones, dispositivos periféricos, soportes de información, así como a las comunicaciones sobre redes abiertas o con cifrado débil, donde se aplican las medidas de seguridad que garanticen que la información se trata acorde a su clasificación.

- **PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS**: PULSIA protege el perímetro de acceso a su sistema, en particular en las conexiones a través de Internet, analizando siempre los riesgos derivados de la interconexión con otros sistemas, y estableciendo las medidas que garanticen el nivel de seguridad necesario.

- **REGISTRO DE ACTIVIDAD**: PULSIA registra las actividades de sus usuarios con el fin de monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello 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.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

- **INCIDENTES DE SEGURIDAD**: Cualquier compromiso de la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información de la empresa se considera un incidente de seguridad. PULSIA dispone de un sistema de detección y reacción frente a los incidentes de seguridad, que son clasificados y gestionados hasta su solución recopilando las evidencias de manera que se pueda informar y aprender de los mismos para mejorar de forma continuada.

  En particular la empresa dispone de un sistema de detección y reacción frente a código dañino, así como de un sistema de prevención y detección de intrusiones, realizando auditorías técnicas para asegurar las medidas de protección pertinentes.

  Los usuarios disponen de canales establecidos para informar de forma inmediata de cualquier incidente o anomalía detectada.

- **CONTINUIDAD DE LA ACTIVIDAD**: PULSIA realiza las copias de seguridad que garantizan la recuperación de la información, y establece los mecanismos adecuados para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

- **PROPORCIONALIDAD**: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

- **MEJORA CONTINUA**: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado.

- **SEGURIDAD POR DEFECTO**: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

  PULSIA considera que las funciones de Seguridad de la Información deberán quedar integradas en todos los niveles jerárquicos de su personal.

  Puesto que la Seguridad de la Información incumbe a todo el personal de PULSIA, esta Política deberá ser conocida, comprendida y asumida por todos sus empleados.

  Para la consecución de los objetivos de esta Política, PULSIA deberá establecer una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su reevaluación. En el transcurso de este ciclo de mejora continua, PULSIA mantendrá la definición tanto del nivel de riesgo residual aceptado (apetito al riesgo) como de sus umbrales de tolerancia.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

4. ALCANCE

El alcance de esta Política de Seguridad de la Información engloba los sistemas de información que soportan los procesos para servicios de:

LOS SISTEMAS DE INFORMACIÓN QUE DAN SOPORTE AL DISEÑO DE INFRAESTRUCTURAS DE RED, DESARROLLO DE SOFTWARE, INSTALACIÓN Y MANTENIMIENTO DE REDES DE ÁREA LOCAL, WAN E INALÁMBRICAS, CONFIGURACIÓN Y MANTENIMIENTO DE EQUIPOS INFORMÁTICOS, SEGURIDAD EN LAS COMUNICACIONES Y SERVICIOS DE CESIÓN DE PERSONAL OUTSOURCING. SEGÚN LA DECLARACIÓN DE APLICABILIDAD.

5. ANÁLISIS Y GESTIÓN DE LOS RIESGOS (ART.14)

La presente Política de Seguridad de la Información es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de la empresa para los procesos descritos.

El personal sujeto a esta Política incluye a todas las personas con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentre esta y de si el individuo es empleado o no de la empresa. Por lo tanto, también se aplica a los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la empresa.

Para garantizar que el proceso de seguridad implantado será actualizado y mejorado de forma continua, se implantará y documentará un Sistema de Gestión de la Seguridad de la Información (SGSI). De esta forma, el contenido de la Política de Seguridad de la Información será desarrollado en normas y procedimientos complementarios de seguridad. La Política deberá estar disponible en la página web corporativa de PULSIA, https://pulsia.es y en un repositorio común de PULSIA, de forma que sea accesible por todas las personas.

Como sabemos, conocer los riesgos y elaborar una estrategia para gestionarlos adecuadamente es primordial para la empresa, ya que únicamente si se conoce el estado de seguridad podrán tomarse las decisiones adecuadas para mitigar los riesgos a los que se enfrenta.

PULSIA utiliza la metodología Magerit para analizar los riesgos, realizando un análisis detallado de los riesgos que afecten a los activos recogidos en un inventario de activos, que queda documentado en un documento de Análisis de Riesgos.

La entidad determina los niveles de riesgo a partir de los cuales toma acciones de tratamiento sobre los mismos. Un riesgo se considera aceptable cuando implantar más

controles de seguridad se estima que consumiría más recursos que el posible impacto asociado.

Una vez llevado a cabo el proceso de evaluación de riesgos, la dirección de la empresa es la responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgo.

6. COMPROMISO DE LA DIRECCIÓN (ART.13)

La Dirección de PULSIA, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre los empleados de PULSIA.
- Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

7. ROLES Y RESPONSABILIDADES (ART.15)

PULSIA se compromete a velar por la Seguridad de todos los activos bajo su responsabilidad mediante las medidas que sean necesarias, siempre garantizando el cumplimiento de las distintas normativas y leyes que le son aplicables.

Para ello, deberán nombrar una figura responsable de definir, implementar y monitorizar las medidas de ciberseguridad y seguridad de la información. Esta figura deberá establecerse desde un entorno de gobierno y gestión, y tendrá entre sus funciones y responsabilidades el aplicar principios de segregación de funciones y el contacto con las autoridades y grupos de interés especiales en materia de seguridad de la información.

Será responsabilidad de esta figura desarrollar y mantener la Política, asegurándose que ésta sea adecuada y oportuna según evolucione tanto la PULSIA como la regulación vigente.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

7.1. Roles, responsabilidades y deberes

Con tal de coordinar los esfuerzos de Seguridad, la organización divide las responsabilidades del personal en tres categorías.

7.1.1. Responsabilidades del usuario

Toda persona o sistema que acceda a la información tratada, gestionada o propiedad de la empresa se considerará un usuario. Los usuarios son responsables de su conducta cuando acceden a la información o utilicen los sistemas informáticos de la empresa. El usuario es responsable de todas las acciones realizadas utilizando sus identificadores o credenciales personales.

Los usuarios tienen la obligación de:

- Cumplir la Política de Seguridad de la Información y las normas, procedimientos e instrucciones complementarias.
- Proteger y custodiar la información de la empresa, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida.
- Conocer y aplicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y el resto de políticas, normas, procedimientos y medidas de seguridad aplicables.

7.1.2. Responsable de la información

El Responsable de la Información es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).

El Responsable de la Información tiene las siguientes responsabilidades:

- Velar por el buen uso de la información y, por tanto, de su protección.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información tratada, valorando las consecuencias de un impacto negativo.

7.1.3. Responsable del servicio

El propietario de los activos del Servicio, entendiendo por tal al responsable de dicho servicio, tendrá las siguientes responsabilidades generales:

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad del servicio, de acuerdo con el Responsable de Seguridad y el Responsable del Sistema.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.

7.1.4. Dirección

La dirección de la empresa está profundamente comprometida con la Política descrita en este documento y es consciente del valor de la información y del grave impacto económico y de imagen que puede producir un incidente de seguridad.

En el contexto del Esquema Nacional de Seguridad, la Dirección asume las responsabilidades descritas para el Responsable de la Información y el Responsable del Servicio.

La Dirección es, por tanto, propietaria de los activos de información propios de PULSIA, y también propietaria de los riesgos.

La dirección asume además las siguientes responsabilidades:

- Demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información.
- Asegurar que se establecen la Política y los objetivos de seguridad de la información y que estos son compatibles con la dirección estratégica de la organización.
- Aprobar y comunicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y la importancia de su cumplimiento a todos los usuarios, internos o externos, a los clientes y a los proveedores.
- Reunirse al menos una vez al año, y cuando cualquier evento o solicitud extraordinaria lo demande, con los Responsables de Seguridad y de Sistemas, para ser informado sobre el SGSI y actualizar la estrategia en materia de Seguridad de la Información.
- Fomentar una cultura corporativa de seguridad de la información.
- Apoyar la mejora continua de los procesos de seguridad de la información.
- Asegurar que están disponibles los recursos necesarios para el cumplimiento de la Política de seguridad de la información, de las normas de uso de los sistemas y para el funcionamiento del sistema de gestión de seguridad de la información.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

- Definir el enfoque para el análisis y la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos y asegurar la evaluación de los mismos al menos con una periodicidad anual.
- Asegurar que se realizan auditorías internas de seguridad de la información y que se revisan sus resultados para identificar oportunidades de mejora.
- Definir y controlar el presupuesto para seguridad de la información.
- Aprobar los planes de formación y las mejoras y proyectos relacionados con la Seguridad de la Información.
- Aprobar la documentación hasta su segundo nivel de normas y procedimientos.
- Determinar las medidas, sean disciplinarias o de cualquier otro tipo, que pudieran aplicarse a los responsables de violaciones de seguridad.

7.1.5. Responsable de Seguridad

La persona con el cargo de Responsable de Seguridad de la Información asumirá las siguientes funciones:

- 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 la Seguridad de la Información 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 Responsables del Servicio y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS, declarando la aplicabilidad de dichas medidas.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
- Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación a las normas especificadas (ENS), en colaboración con el Responsable de Sistemas.
- Realizar con la colaboración del Responsable del Sistema, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo.
- Asimismo, junto al Responsable del Sistema, aceptar los riesgos residuales calculados en el análisis de riesgos.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

- 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 al Responsable del Sistema para que adopte las medidas correctoras adecuadas. Coordinar el proceso de Gestión de la Seguridad, en colaboración con el Responsable de Sistemas.
- Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
- Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el Responsable de Sistemas.
- 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 lo previsto en el Anexo II del ENS.
- Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, en coordinación con el Responsable del Sistema, aportando información puntual para la toma de decisiones.
- Responsable de la ejecución directa o delegada de las decisiones de la Dirección, se reunirá con esta y con el Responsable del Sistema, al menos con una frecuencia anual, para asegurar la estrategia.
- Respecto a la documentación, y apoyándose en el Responsable del Sistema, son funciones del Responsable de Seguridad:
- Proponer a la Dirección y al Responsable de Sistemas para su aprobación la documentación de seguridad de segundo nivel (Normas de Seguridad TIC –TIC– y Procedimientos Generales del Sistema de Gestión de la Seguridad de la Información –SGSI–) y firmar dicha documentación.
- Aprobar la documentación de seguridad de tercer nivel (Procedimientos Instrucciones Técnicas STIC).
- Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.
- Para el desarrollo de cualquiera de sus funciones el Responsable de Seguridad podrá recabar la colaboración del Responsable del Sistema.
- Tipo documentación
- Información

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

7.1.6. Delegado de protección de datos

Siguiendo lo indicado en el RGPD y en la LOPDGDD, el Delegado de Protección de Datos tendrá como mínimo las siguientes funciones:

- Informar y asesorar al responsable del tratamiento y a sus empleados de las obligaciones que les incumben en relación al RGPD y otras disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado 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.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Tipo documentación
- Información

7.1.7. Responsable del Sistema

Serán funciones del Responsable del Sistema las siguientes:

- Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

- Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el Responsable de Seguridad.
- 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 Responsable de Seguridad y la Dirección.
- Realizar con la colaboración del Responsable de Seguridad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable de Seguridad, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Elaborar en colaboración con el Responsable de Seguridad, la documentación de seguridad de tercer nivel (Procedimientos Operativos STIC e Instrucciones Técnicas STIC).
- 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 de los sistemas de información.
- La gestión de las autorizaciones concedidas a los usuarios 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 operativos de seguridad.
- Aplicar los cambios de configuración del sistema de información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente, así como 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 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.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

- Informar a los respectivos Responsables 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.

7.1.8. Comité de Seguridad de la Información

Compuesto por el responsable del sistema, la dirección y la responsable administrativa, se reúne al menos semestralmente para coordinar la seguridad de la información a nivel de la organización.

El Comité de Seguridad de la Información asume las responsabilidades del Responsable de Seguridad, además de las funciones siguientes:

- Atender las inquietudes de la dirección y de sistemas.
- Obtener una fotografía del estado de la seguridad de la información.
- Promover la mejora continua del SGSI.
- Elaborar la estrategia de evolución.
- Revisar la Política, Normativa y procedimientos al menos anualmente.
- Aprobar los requisitos de formación.
- Priorizar actuaciones
- Promover la realización de auditorías del SGSI y técnicas.
- Comprobar que la Seguridad de la Información está presente en todos los proyectos.

8. ANÁLISIS Y GESTIÓN DE LOS RIESGOS (ART.14)

La presente Política de Seguridad de la Información es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de la empresa para los procesos descritos.

El personal sujeto a esta Política incluye a todas las personas con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentre esta y de si el individuo es empleado o no de la empresa. Por lo tanto, también se aplica a los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la empresa.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

Para garantizar que el proceso de seguridad implantado será actualizado y mejorado de forma continua, se implantará y documentará un Sistema de Gestión de la Seguridad de la Información (SGSI). De esta forma, el contenido de la Política de Seguridad de la Información será desarrollado en normas y procedimientos complementarios de seguridad. La Política deberá estar disponible en la página web corporativa de PULSIA, www.pulsia.es y en un repositorio común de PULSIA (Sharepoint), de forma que sea accesible por todas las personas.

Como sabemos, conocer los riesgos y elaborar una estrategia para gestionarlos adecuadamente es primordial para la empresa, ya que únicamente si se conoce el estado de seguridad podrán tomarse las decisiones adecuadas para mitigar los riesgos a los que se enfrenta.

PULSIA utiliza la metodología Magerit para analizar los riesgos, realizando un análisis detallado de los riesgos que afecten a los activos recogidos en un inventario de activos, que queda documentado en un documento de Análisis de Riesgos.

La entidad determina los niveles de riesgo a partir de los cuales toma acciones de tratamiento sobre los mismos. Un riesgo se considera aceptable cuando implantar más controles de seguridad se estima que consumiría más recursos que el posible impacto asociado.

Una vez llevado a cabo el proceso de evaluación de riesgos, la dirección de la empresa es la responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgo.

9. COMPROMISO DE LA DIRECCIÓN (ART.13)

La Dirección de PULSIA, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre los empleados de PULSIA.
- Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

10. CLASIFICACIÓN DE LA INFORMACIÓN

10.1. Niveles de clasificación

NIVEL	DETALLE NIVEL	EJEMPLOS
General	Se trata de la información que puede ser conocida por cualquier tipo de persona y su utilización fraudulenta no supone un riesgo para los intereses de PULSIA.	Son ejemplos de este tipo de información los catálogos de productos y la información disponible en la página Web.
Restringido	Es la información utilizada por las áreas De PULSIA y cuya utilización fraudulenta supone un riesgo para los intereses del Grupo poco significativo.	Son ejemplo de este tipo de información los correos electrónicos y los documentos de trabajo de las áreas del grupo.
Confidencial	Es aquella información que solo puede ser conocida por un número reducido de personas y para la que un uso fraudulento puede suponer un impacto para los intereses de PULSIA significativo.	Son ejemplos de este tipo de información los informes de auditoría y de estrategia del grupo.

10.2. Gestión de información privilegiada

La información que se considere reservada, confidencial o secreta se deberá tratar con especial cuidado, debiéndose definir medidas de seguridad extraordinarias o adicionales para el adecuado tratado de esta.

Este tipo de información se deberá enviar cifrada y mediante protocolos seguros.

Tipo documentación

Información

10.3. Etiquetado de la información

PULSIA deberá etiquetar mediante métodos manuales o, en la medida de lo posible, automatizados para facilitar el procesamiento adecuado de las medidas de seguridad que apliquen en cada caso.

Se deberán etiquetar los documentos o materiales, así como los anexos, copias, traducciones o extractos de estos, según los niveles de clasificación de la información exceptuando la información considerada de “Uso público”.

Se deberá definir un proceso o procedimiento para el etiquetado de la información de acuerdo con los siguientes requisitos:

- Asegurar que el etiquetado de la información refleja el esquema de clasificación de la información adoptado.
- Asegurar que las etiquetas sean fácilmente reconocibles entre los empleados.
- Orientar a los empleados sobre dónde y cómo se colocarán o utilizarán las etiquetas, en función del proceso de acceso a la información o a los activos que la soportan.
- Indicar las excepciones en los que se permite omitir el etiquetado, sin que ello suponga una omisión del deber de clasificar la información.

Se deberá prestar especial atención y tratar con cuidado máximo el etiquetado de activos físicos que contengan información reservada o secreta, para evitar su sustracción por ser fácilmente identificable.

Tipo documentación

Información

10.4. Manipulación de la información

PULSIA se encargará de desarrollar e implementar un conjunto adecuado de procedimientos para la correcta manipulación la información. Se deberán adoptar las medidas necesarias para proteger la información de acuerdo a su clasificación, de forma que la información confidencial o secreta estará en todo momento custodiada durante todo el ciclo de vida de la misma.

10.5. Privacidad de la información

PULSIA deberá asegurar la privacidad de los datos de carácter personal con el objetivo de proteger los derechos fundamentales de las personas físicas, especialmente su derecho al honor, intimidad personal y familiar y a la propia imagen, mediante el establecimiento de medidas para regular el tratamiento de los datos. De esta forma cumplirá con la legislación vigente en materia de protección de datos personales en función de la jurisdicción en la que esté establecida y opere (a modo ilustrativo, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantías de los Derechos Digitales para el caso de España) y deberá incluir las medidas necesarias para cumplir con la normativa.

Se deberán implementar medidas adecuadas para asegurar la privacidad de la información en todas las fases de su ciclo de vida.

Tipo documentación

Información

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

10.6. Prevención de fugas de información

La fuga de información es una salida no controlada de información (intencionada o no intencionada) que provoca que la misma llegue a personas no autorizadas o que su propietario pierda el control sobre el acceso a la misma por parte de terceros.

Se deberán analizar los vectores de fuga de información. Para ello, se deberán identificar los activos cuya fuga supone mayor riesgo, basándose en la criticidad del activo y el nivel de clasificación que la información tenga. Además, se deberán identificar las posibles vías de robo, pérdida o fuga de cada uno de los activos en sus diferentes estados del ciclo de vida.

PULSIA deberá definir procedimientos para evitar la ocurrencia de las situaciones que puedan provocar la pérdida de información, así como procedimientos de actuación en caso de que se notifique una fuga de información.

Se deberá asegurar la formación y capacitación de todos los empleados en torno a buenas prácticas para la prevención de fugas de información. Especialmente se deberán tener en cuenta, al menos, los siguientes aspectos:

- Proceso para el manejo de dispositivos de alta criticidad conocidos.
- Uso adecuado de dispositivos extraíbles como USBs, CD/DVDs o similares.

11. POLÍTICAS DE SEGURIDAD DEL PERSONAL (ART.17-18)

Se han diseñado unas políticas que deben ser llevadas a cabo a la hora de acceder a la información de la organización y que responden a la siguiente clasificación.

11.1. De la instalación del equipo informático

Todo el equipo informático (PCs, servidores, teléfonos móviles, PDA, otros dispositivos...), que corresponda al uso exclusivo de personal contratado por la Organización está sujeto a las normas y procedimientos de instalación de PULSIA bajo supervisión del Responsable de Seguridad de la Organización o el personal designado por éste. La instalación de cualquier programa deberá disponer de autorización por su parte.

Los equipos de la organización destinados a funciones de propósito específico y vinculados a servicios de carácter crítico deberán alojarse exclusivamente en la infraestructura del proveedor de hosting contratado. Dicho proveedor deberá garantizar Las condiciones ambientales, la alimentación eléctrica y su acceso está regulado mediante los mecanismos oportunos.

Los usuarios de los equipos de uso personal deberán responsabilizarse de cumplir con las políticas de seguridad establecidas por PULSIA.

Los responsables de las distintas áreas de los departamentos con personal y acceso a la información de la organización deberán en conjunción con el Responsable de Seguridad dar cumplimiento con las normas de instalación y notificaciones correspondientes de actualización, reubicación, reasignación, adjudicación, etc., tanto del personal como de los equipos de uso exclusivo del mismo.

11.2. Del mantenimiento del equipo informático

Cada equipo destinado en exclusiva al trabajo para la organización, aun perteneciendo a una entidad externa, será responsabilidad de la persona a la que haya sido asignado, por lo que cualquier cambio en el puesto de trabajo y/o de cualquier PC y material de la organización deberá ser registrado.

El acceso desde ordenadores portátiles y otros dispositivos móviles a la información de la organización (para consultorías externas, asesorías, etc.) se hará solicitando el mismo al Responsable de Seguridad, el cual otorgará un acceso temporal a los recursos necesarios de la organización con la finalidad con que se disponga, comprometiéndose el usuario de dicho dispositivo a no mantener ninguna copia en local de dicha información y cumplir con los normas establecidas para el acceso a la misma expuestas en este documento.

Tipo documentación

Información

11.3. Del control de acceso al equipo informático

Todos y cada uno de los equipos son asignados a un usuario, por lo que es de su competencia hacer buen uso de estos. Cada trabajador se encargará de llevar a cabo las siguientes prácticas de Seguridad recomendadas en su equipo:

- El acceso a los equipos se realizará mediante cuentas locales autorizadas y regirse por las normas en cuanto a política de contraseñas de la organización.
- Apagar el ordenador fuera del horario de trabajo, así como evitar el uso de este por terceras personas.
- Proteger el escritorio de este durante las ausencias del puesto de trabajo en horario de oficina, mediante el bloqueo del PC. Los equipos se configuran con protección por contraseña que se activa tras un período de inactividad.
- No revelar las contraseñas personales a nadie, no registrarlas en ningún soporte que no garantice la correcta protección de estas como, por ejemplo, soporte papel.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

- Emplear el correo proporcionado por la organización de una manera responsable y siempre únicamente en el ámbito profesional, evitándose hacer uso de ella en para el ámbito privado. No emplear recursos productivos facilitados por PULSIA, para usos no pertinentes.
- Comunicar cualquier incidencia de seguridad (posible virus, comportamientos sospechosos, etc.) al responsable de Seguridad.

El acceso a información corporativa se realizará a través de la red de datos corporativa, así como el acceso a datos corporativos, el cual estará limitado a los usuarios que deban usarla mediante autenticación por nombre de usuario y contraseña.

11.4. Política de contraseñas

- Todos los empleados que necesitan acceso a algún Sistema de Información de la organización disponen de un Identificador ID de usuario único y una contraseña personal.
- El usuario asociado a cada empleado será conforme a los privilegios que corresponden a sus funciones, responsabilidades y actividades.
- Todos los usuarios son responsables de proteger sus identificadores de usuario y contraseñas.
- Las contraseñas escogidas por los usuarios deben ser difíciles de adivinar y no deben contener información relacionada con su trabajo y su vida personal: números de teléfono, nombre de familiares, direcciones, números personales (PIN, SIN, DNI, etc.), lugares conocidos, etc.
- Las contraseñas deben ser cambiadas con la periodicidad y cumplir las normas establecidas para cada sistema.
- Las contraseñas no deben ser almacenadas en ficheros legibles, macros, PCs sin control de acceso o ningún otro lugar donde puedan ser accedidas por personas sin autorización.
- Los administradores del sistema y personal técnico nunca solicitarán la contraseña a sus usuarios. La única excepción es la asignación inicial de la contraseña personal con el compromiso por parte del usuario de cambiarla inmediatamente en el primer acceso al sistema.
- Si un usuario sospecha que su identificador y contraseña está siendo utilizado ilegalmente, es su responsabilidad avisar inmediatamente al responsable de Seguridad.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

11.5. Del control del soporte en papel

Dado que la organización no emplea soporte en papel en su operativa habitual, los empleados deberán extremar la protección de la información digital, evitando dejar datos confidenciales visibles, accesibles o desatendidos en sus dispositivos durante las sesiones de teletrabajo. Asimismo, deberán bloquear la pantalla cuando se ausenten del puesto y garantizar que no existan copias locales no autorizadas ni descargas innecesarias que comprometan la seguridad de la información.

11.6. Del control de acceso remoto y teletrabajo

La organización dispone de una conexión remota a su red para usuarios en su puesto de teletrabajo. La conexión remota se realiza de forma cifrada para autenticarse. El usuario remoto se compromete a adoptar las medidas de Seguridad en su equipo para garantizar que el acceso a los datos se realiza de manera responsable.

El equipo utilizado para la conexión en la modalidad de trabajo en remoto será proporcionado por PULSIA y dispondrá de los siguientes requerimientos de seguridad.

- Capacidad de realizar una conexión a través de una VPN.
- Disponer de un sistema operativo actualizado con los últimos parches y actualizaciones
- de seguridad.
- Software antivirus instalado.
- Software de firewall/cortafuegos personal instalado.

El servicio de teletrabajo se monitorizará y controlará, registrándose tanto la conexión como la actividad de acuerdo con los protocolos de seguridad.

11.7. Del acceso a Internet

Los accesos a Internet a través de los navegadores deben sujetarse a las normas éticas y es responsabilidad de cada usuario realizar un uso lícito de los medios de que le provee la organización para el correcto desempeño de su trabajo.

El acceso web a la Intranet de la organización se realizará desde cualquier puesto de trabajo y es protegido mediante el control de accesos. Por ello, toda la programación involucrada en la tecnología Web deberá cumplir unos requisitos de calidad y de seguridad.

El material que aparezca en la página web deberá ser aprobado por Gerencia, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

11.8. De la utilización de los recursos de Pulsia

Todos los empleados que utilicen los Sistemas de Información de la organización deben firmar la aceptación de esta política de Seguridad. Al firmar esta política, el empleado acepta comprender y comprometerse al cumplimiento de las políticas y procedimientos de la organización relativas al uso de los Sistemas de Información, incluyendo las normas de la presente política.

El uso del correo electrónico para comunicaciones corporativas estará limitado a las cuentas de la organización y deberá cumplir con el propósito del desempeño del trabajador.

La cesión de datos a través de este medio deberá estar autorizada para la finalidad exclusiva para la cual sea necesario. Está prohibido copiar, sin justificación o autorización, información propia de la organización o software.

Aquellos responsables de reenvío de información a terceros sin autorización estarán sujetos a la aplicación de medidas disciplinarias. Incluido en este apartado está la prohibición de enviar cartas o solicitudes, así como transmitir cualquier software no validado por la organización.

Se hará un uso responsable de otras cuentas personales para uso particular en la organización. Además, será responsabilidad del usuario la apertura de mensajes de correo, por lo que se aconseja no abrir correos electrónicos no solicitados, de remitentes desconocidos o sospechosos. Es responsabilidad igualmente del usuario el buen uso del correo electrónico, si bien se dispondrán las medidas técnicas por parte de PULSIA para evitar el spam de correo, las cuentas no autorizadas, etc. Debido a que las cuentas de correo electrónico corporativas son cedidas por la organización para uso profesional del empleado, el usuario deberá atenerse a las reglas establecidas para su uso por la organización.

11.9. De la utilización de soportes de información

Se prohíbe expresamente la salida de soportes de información extraíble (dispositivos de almacenamiento USB, memorias flash, etc.) con datos confidenciales o restringidos de PULSIA, sin el consentimiento expreso del Responsable de Seguridad y con las medidas de seguridad adecuadas. Cuando se usen dichos dispositivos dentro de PULSIA,

los usuarios deben ser conscientes de ejecutarlos solo en equipos con antivirus actualizados y conocer perfectamente el origen de dicho medio y que sea confiable.

Cualquier información que sea almacenada en un soporte de información extraíble deberá ser empleada exclusivamente para motivos de trabajo y la información deberá eliminarse de manera segura o guardarse bajo llave una vez deje de ser útil.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

11.10. De supervisión y evaluación

La organización se reserva el derecho de monitorizar e inspeccionar el correcto uso de los Sistemas de Información por parte de los empleados en cualquier momento, respetando la legislación vigente en cuanto al derecho de privacidad de los empleados. Estas comprobaciones pueden llevarse a cabo con o sin el consentimiento y presencia del empleado involucrado y se llevarán a cabo con el consentimiento expreso del responsable de la Gerencia.

Periódicamente se realizará un escaneo en la red empleada por PULSIA, en busca de posibles fallos y vulnerabilidades, así como de virus en los PCs, servidores y recursos de la organización y una actualización del inventario de aplicaciones y uso de los recursos de cada PC.

Con una periodicidad mínima anual se revisará esta política de Seguridad para adecuarla a los posibles cambios en la organización o legislativos y se analizarán las incidencias y no conformidades encontradas en el sistema, elaborando una lista de acciones a emprender y ejecutar durante el año siguiente para garantizar la Seguridad y el buen uso de los recursos de la Organización. Como excepción se encuentran los sistemas considerados críticos que estarán bajo monitorización permanente.

Se realizarán las copias de Seguridad y recuperación de ficheros según las normas establecidas en los procedimientos correspondientes.

Cualquier incidencia acaecida en los sistemas de información será registrada y se gestionará según las normas establecidas en los procedimientos correspondientes. Las incidencias que afecten a la RGPD / LOPDGDD, serán marcadas como tales.

Periódicamente se llevará a cabo por parte de una tercera organización la auditoría de cumplimiento del RGPD (“Reglamento General de Protección de Datos”) y de la LOPDGDD (“Ley Orgánica de Protección de Datos”), así como auditorías del Sistema de Gestión de la Seguridad de la Información (SGSI).

11.11. Propiedad intelectual el material desarrollado en la organización

PULSIA tiene derechos exclusivos sobre patentes, copyrights, licencias, desarrollos y cualquier otra propiedad intelectual desarrollada por sus empleados con motivo de su trabajo en PULSIA. Además, todos los desarrollos y documentos producidos o provistos por los empleados para el propósito de la organización son propiedad de PULSIA quien se reserva el derecho de acceso y utilización de esta documentación en virtud de los intereses de la organización.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

12. POLÍTICAS DE ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD (ART.19)

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 de este real decreto, 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.

El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

- Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
- Otras certificaciones de seguridad adicionales que se requieran normativamente.
- Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

13. MÍNIMO PRIVILEGIO (ART.20)

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

- El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- 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.
- 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

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

- 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.

14. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA (ART.21)

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

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. La Responsabilidad será a cargo del responsable de seguridad de PULSIA.

15. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO (ART.22)

En la organización e implantación de la seguridad se 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.

16. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS (ART.23)

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

17. REGISTRO DE LA ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO (ART.24)

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, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán 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 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, los sujetos comprendidos en el artículo 2 podrán, 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.

18. INCIDENTES DE SEGURIDAD (ART.25)

La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero , por el que se

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

19. CONTINUIDAD DEL NEGOCIO (ART.26-27)

Respondiendo a requerimientos de calidad y buenas prácticas, PULSIA deberá disponer de un Plan de Continuidad de Negocio como parte de su estrategia para garantizar la continuidad en la prestación de sus servicios esenciales o críticos y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para que la sociedad actúe en caso de ser necesario. Este Plan de Continuidad deberá ser actualizado y aprobado periódicamente. Además, se deberá definir y mantener actualizado un Plan de Recuperación ante Desastres alineado con la continuidad de negocio. Este plan abarcará la continuidad del funcionamiento de las tecnologías de información y comunicación.

PULSIA deberá encargarse de la formación y capacitación para todos sus empleados en materia de Continuidad del Negocio, la cual deberá ser revisada periódicamente con el objetivo de estar totalmente alineada con el Plan existente.

20. CUMPLIMIENTO REGULATORIO

PULSIA deberá comprometerse a dotar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se velará por el cumplimiento de toda legislación, normativa o regulación aplicable.

21. REVISIÓN Y AUDITORÍAS

El responsable de seguridad revisará esta Política anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por la dirección. Las revisiones comprobarán la efectividad de la Política, valorando los efectos de los cambios tecnológicos y de negocio. La dirección será responsable de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a las situaciones de riesgo establecidas en el presente documento.

El sistema de gestión de seguridad se auditará cada año, según un plan de auditorías.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

22. SGSI

El SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

22.1. Infraestructura Pulsia

La infraestructura de la organización consta de un conjunto de servicios que pueden ser gestionados internamente o delegado en terceros (proveedores). Dichos servicios serán agrupados en las distintas áreas de la organización que contarán con perfiles diferenciados para el acceso a los recursos de la organización y su forma de consumirlos.

22.2. Áreas de la organización

Se listan a continuación las diferentes áreas de la organización. Cada área podrá tener servicios compartidos con otras áreas y servicios de acceso específico. De este modo se establece una arquitectura que permite segmentar los servicios para acceder de manera controlada a los mismos.

- Negocio
- Administración
- Comercial
- RRHH
- Desarrollo
- Microinformática
- Sistemas
- Externos (Clientes)
- Alumnos de Prácticas

Por ejemplo, se debe garantizar que mientras todas las áreas compartirán el acceso al servicio de correo electrónico sólo los miembros del área de "administración" deben acceder en exclusiva al software de gestión y facturación.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es

22.3. Servicios de la organización

Una vez garantizados los accesos lícitos a los diferentes servicios que consume cada área, proporcionados por la propia organización o delegados en terceros, se debe establecer un acceso granular del servicio, de modo que, existan perfiles con diferentes grados de acceso. Además, existirán servicios cuyo acceso debe estar controlado y requerirán autenticación.

Ejemplos de servicios pueden ser: Correo, LDAP, VPN, Documentación, Contabilidad, Facturación, Gestión, Pulsia Ticketing, GIT, Keepass/Bitwarden, Web, IONOS, StackScale, GLPI… se pueden consultar los servicios disponibles (según credenciales) desde el apartado de aplicaciones.

22.4. Inventario

Principales elementos de la infraestructura. Consultar inventario.

22.5. Análisis de Riesgos

Acceso al documento de Análisis de Riesgos.

22.6. Entorno virtualizado

Para dar solución a los requisitos de la organización se establece una arquitectura virtualizada en la nube. Esta arquitectura se provee por StackScale y se compone de un entorno gestionado con el software VSphere del fabricante de software VMWare. El entorno se compone de 3 nodos físicos de computación y un almacenamiento de datos. Estos se interconectan mediante dos switches físicos (que proporcionan alta disponibilidad) y un switch virtual.

Dicha infraestructura da soporte a los diferentes servicios que corren en máquinas virtualizadas dentro del entorno. Las máquinas se segmentan en diferentes zonas y redes en función de los servicios que sirven.

- La política por defecto es **Denegar** el tráfico entre las zonas y redes.
- De este modo se establecen zonas atendiendo a los siguientes criterios:
- WAN, zona dedicada al tráfico proveniente de internet
- LAN, incluye las redes definidas más abajo y nuevamente segmentadas en base a los criterios específicos (excepciones de reglas)
- VPN, Tráfico cifrado entrante y saliente
- DMZ, enlace de alta disponibilidad entre firewalls (aislado a nivel de enlace)

- De este modo se establecen redes atendiendo a los siguientes criterios:
- **Red de producción**, alberga máquinas que serán accesibles públicamente por cualquier usuario.
- **Red de desarrollo**, alberga máquinas que contienen los desarrollos de códigos fuentes de la empresa. Será accesible únicamente bajo VPN para los usuarios del grupo "desarrollo".
- **Red de servicios**, alberga máquinas que proporcionan servicios para la propia organización (LDAP, Radius). Estos servicios son usados por otras aplicaciones, pero nunca se deben de acceder directamente.
- **Red de empleados**, servicios de la organización sólo disponibles bajo VPN
- **Red de externos**, alberga máquinas que proporcionan servicios para clientes y personal externo. Requiere acceso VPN y/o control de ip origen.

REGLAS

ORIGEN	DESTINO	REGLA
WAN	Red producción	80, 443, 10051 HTTP, HTTPS, ZABBIX, ACTIVO
Red producción	WAN	53, 80, 443, 25, 465, 587, 995, 110, 143, 993 DNS, HTTP, HTTPS, POP, SMTP, IMAP
Red desarrollo [Máquina Salto]	Red producción	22 [1] SSH
Red producción	Red Servicios	LDAP [2] ZABBIX ACTIVO [3]
	Red Servicios	GLPI [4] ZABBIX INTER. TRAPPER [7]
Red Servicios	*	ZABBIX PASIVO [5]
VPN	WAN	53, 80, 443, 25, 465, 587, 995, 110, 143, 993, 22 [6] DNS, HTTP, HTTPS, POP, SMTP, IMAP
VPN	Red desarrollo [Máquina de Salto]	Rol Desarrollo

VPN	Red Servicios	Rol Sistemas
VPN	Red Servicios	DNS
VPN	Red desarrollo [Máquina de Salto]	Rol Devops
VPN [Rol Desarrollo, RRHH, Devops]	Red producción	HTTP
VPN	Red producción	Rol Sistemas

[1] Objetivo: Sólo los usuarios DevOps podrán "mover" datos desde la red de producción a la red de desarrollo. Para ello se usará una máquina de salto. Ninguna máquina de la red de desarrollo tendrá acceso a la red de producción a excepción de esta máquina. Para evitar que sea usada como bypass del acceso controlado, no se permitirá ningún tráfico a esta máquina distinto al acceso vía RDP [3389] usando la conexión desde VPN por usuarios de rol DevOps. Se establecerá una regla local en la máquina de salto para denegar el acceso desde cualquier máquina de la misma red.

[2] Crear un usuario para usar el servicio de LDAP desde producción. Para evitar que una vulnerabilidad de la máquina de Pro permita obtener los datos del LDAP. Limitar la máquina origen por IP.

[3] El servicio de correo es el encargado de mandar datos como la cola de envío que debe ser reportado por el agente en modo activo. El resto de los servicios pueden ser pasivos

[4] Servicio de inventariado mediante API. OCS -> GLPI

[5] El agente Zabbix no envía la información si no el servidor es el que inicia la conexión para recabar los datos (pulling)

[6] Para la conexión SSH mediante IP pública de Pulsia [VPN] a otros sistemas de clientes. Ej.: Alcobendas

[7] Algunos servicios deben enviar de forma activa información al servidor Zabbix Interno.

Pulsia ® | C/Biología 12, Edificio Vilamar II, Planta 2 Oficina 3, 41015 Sevilla | info@grupopulsia.es