1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 01 de Marzo de 2024 por Pablo Barrachina Tortajada.

Esta Política de Seguridad de la Información es efectiva desde esta fecha y hasta que sea reemplazada por una nueva Política. Ha sido publicada en el día de hoy en la Intranet de la Compañía y todos los trabajadores han sido informados de ello.

2. INTRODUCCIÓN

DIGITAL VALUE S.L. 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 o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

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

Los diferentes responsables deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

La política de seguridad aborda el SGSI desde las cinco dimensiones DICAT siguiendo las mejores prácticas del sector.

● **Disponibilidad**: Capacidad del sistema de seguir funcionando independientemente de los acontecimientos externos.
● **Integridad**: Garantizar que la información no sea alterada sin autorización.
● **Confidencialidad**: Asegurar que solo pueda acceder a la información los destinatarios autorizados
● **Autenticidad**: Asegurar que la información, su autoría y publicación sea auténtica y no sea suplantada.
● **Trazabilidad**: Registro de las operaciones que permita que la operación pueda ser rastreada hasta su origen.

2.1. PREVENCIÓN

Los responsables deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 8 del ENS.

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

2.3. RESPUESTA

Los responsables de los servicios deben:

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

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los responsables deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

DIGITAL VALUE es una consultora tecnológica especializada en implantación de soluciones para la transformación digital de la administración pública local. Nuestra misión es implantar servicios digitales, y en la nube, basados en tecnologías Web, que aporten soluciones sencillas pero eficaces para la Comunicación, Transparencia y Participación Municipal.
Nuestras Soluciones Web y de Correo Electrónico para Ayuntamientos incluyen los de servicios de Hosting, DataCenter y Administración completa de Sistemas. Todos estos procesos se desarrollan sujetos a esta Política lo que asegura la Confidencialidad, Disponibilidad, Integridad, Autenticidad y Trazabilidad de la información que se gestiona en la organización.

Esta política se aplica a todos los sistemas TIC de DIGITAL VALUE S.L. y a todos los miembros de la organización, sin excepciones.

4. MISIÓN

El objetivo de la seguridad de la información es asegurar la continuidad del negocio y la seguridad de la información de los activos de DIGITAL VALUE S.L. para ello, los objetivos a seguir son los siguientes:

- Identificar, clasificar y valorar los activos dentro de la empresa.
- Analizar y determinar el valor del riesgo existente en los procesos de la empresa.

- Implementar controles para fortalecer las estrategias de seguridad y determinar el valor del riesgo existente en los procesos de la empresa.
- Lograr que toda la organización se conciencie de la importancia de la seguridad de la información.

En DIGITAL VALUE S.L. se ha entendido como fundamental para que el sistema sea efectivo y garantizar la mejora continua del mismo la participación y compromiso de todo el personal de la empresa.

5.- PRINCIPIOS BÁSICOS

Esta política de seguridad se establece de acuerdo con los principios básicos señalados en el capítulo II y se desarrolla aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de la actividad y detección de código dañino.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
ñ) Mejora continua del proceso de seguridad.

Estos requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, del RD 311/2022, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos.

6.- MARCO NORMATIVO

DIGITAL VALUE se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes:

Normativa del Sector Público

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se trasponen al ordenamiento jurídico española las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 2/2015, de 2 de abril, de la Generalitat, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana.
- Ley 38/2003, de 17 de noviembre, General de Subvenciones

Normativa relativa a la Seguridad de la Información

- Reglamento 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Otras Normativas

- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Ley 18/2018, de 13 de julio de la Generalitat Valenciana, para el fomento de la responsabilidad social.
- Los distintos convenios que sean de aplicación a la organización y que se encuentren en vigor.
- El estatuto de los trabajadores que se encuentre en vigor.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

7.- ORGANIZACIÓN DE LA SEGURIDAD

7.1.- COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad de la Información estará formado por los miembros indicados en el apartado 6.2.

El Secretario del Comité de Seguridad TIC será el Responsable de Seguridad y tendrá como funciones:

- Convocar al Comité de Seguridad TIC, recopilando la información pertinente.
- Ser responsable, junto con los diferentes responsables de seguridad delegados, en su caso, de estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que puedan afectar directa o indirectamente a la seguridad de los sistemas de información de la Corporación, debiendo informarse de las consecuencias para las actividades de la Organización, alertando al Comité de Seguridad TIC y proponiendo las acciones oportunas de adecuación al nuevo marco normativo.
- Ser el responsable de la toma de decisiones día a día entre las reuniones del Comité de Seguridad TIC. Estas decisiones estarán presididas por los principios de unidad de acción y coordinación de actuaciones en general y, en especial, en caso de incidencias que tengan repercusión fuera de la organización y en caso de desastres.

El Comité de Seguridad TIC tendrá las siguientes funciones:

- Coordinar todas las funciones de seguridad de los sistemas de información TIC de la Corporación.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Proponer las modificaciones o revisiones de la presente Política de Seguridad que considere oportunas.
- Recabar del Responsable de Seguridad informes regulares del estado de la seguridad de la Organización y de los posibles incidentes.
- Coordinar y dar respuesta a las inquietudes transmitidas a través del Responsable de Seguridad.
- Dinamizar la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas de información, promoviendo inversiones de carácter horizontal.
- En caso de conflicto entre las diferentes figuras de naturaleza unipersonal que componen la estructura organizativa, prevalecerá la decisión del Comité de Seguridad TIC.
- Designar los cargos que componen el comité cada dos años.
- Garantizar la celebración de sesiones de concienciación, por parte del Responsable de Seguridad, del personal en materia de seguridad.
- Y cualesquiera otros cometidos que les sean encargados por la presente Política y por la Dirección de la Corporación.

El Comité de Seguridad TIC se reunirá con carácter ordinario, como mínimo una vez al año. Por razones de urgencia podrá reunirse siempre que algún miembro del Comité lo estime conveniente.

7.2.- ROLES: FUNCIONES Y RESPONSABILIDADES

Atendiendo a las indicaciones de las guías CCN STIC 801 y 805 se diferenciarán los siguientes roles responsables de la seguridad de los sistemas de información:

- **Responsable de la información**: determina los requisitos de la información tratada.
- **Responsable del servicio**: determina los requisitos de los servicios prestados.
- **Responsable de la seguridad** (STIC): determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- **Responsable del sistema** (TIC): a nivel operacional, desarrolla y mantiene el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- **Administrador de sistemas** (ASS): se encarga, a nivel de ejecución, de la implementación y mantenimiento de las medidas de seguridad aplicables necesarias así como la gestión del Sistema de Información.

Responsable de la información	Pablo Barrachina Tortajada
Responsable del servicio	Francisco Sobrevela Pérez
Responsable de la seguridad (STIC)	Pablo Barrachina Tortajada
Responsable del sistema	Pablo Barrachina Santana
Responsable de Sistemas	Ivan Mykhats

Como se puede apreciar en la distribución de los cargos anteriores, se cumple la segregación de funciones definida en el artículo 11 del ENS (el Responsable de la Seguridad no puede ser ni el Responsable del Servicio ni el Responsable del Sistema).

A continuación se especifican las tareas de seguridad y los responsables involucrados en las mismas:

Tarea	**Responsable**
Determinación de los niveles de seguridad requeridos en	R. INFO + R. SERV

cada dimensión	*(Dirección)*
Determinación de la categoría del sistema	RSEG *(Supervisión)*
Análisis de riesgos	RSEG *(Supervisión)*
Declaración de aplicabilidad	RSEG *(Supervisión)*
Medidas de seguridad adicionales	RSEG *(Supervisión)*
Configuración de seguridad	**elabora**: RSEG *(Supervisión)* **aplica**: RDO *(Operación)*
Implantación de las medidas de seguridad	RDO *(Operación)*
Aceptación del riesgo residual	R. INFO + R. SERV *(Dirección)*
Documentación de seguridad del sistema	RSEG *(Supervisión)*
Política de seguridad	**elabora**: RSIS *(Supervisión)* **aprueba** : Dirección
Normativa de seguridad	**elabora**: RSIS *(Supervisión)* **aprueba**: Dirección
Procedimientos operativos de seguridad	**elabora**: RSIS *(Operación)* **aprueba**: RSEG *(Supervisión)* **aplica**: RDO *(Operación)*
Estado de la seguridad del sistema	**monitoriza**: RDO *(Operación)* **reporta**: RSEG *(Supervisión)*

A continuación se precisan mediante una matriz RACI cada una de las tareas que deben llevar a cabo los responsables.

	Rol	**Descripción**
R	**Responsible**	Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista sólo un R, si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RASCI. Es quien debe ejecutar las tareas.
A	**Accountable**	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las tareas.
C	**Consulted**	Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información

		(comunicación bidireccional).
I	**Informed**	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

	Dirección	**Supervisión**	**Operación**
Tarea	**R.INFO + R.SERV**	**R. SEG**	**R. SIS + RDO**
niveles de seguridad requeridos por la información de correo electrónico	A	R	C
niveles de seguridad requeridos por la información de alojamiento web	A	R	C
niveles de seguridad requeridos por el servicio de correo electrónico	A	R	C
niveles de seguridad requeridos por el servicio de alojamiento web	A	R	C
determinación de la categoría del sistema	I	A/R	I
análisis de riesgos	I	A/R	C
declaración de aplicabilidad	I	A/R	C
medidas de seguridad adicionales		A/R	C
configuración de seguridad	I	A	R
aceptación del riesgo residual	A	R	I
documentación de seguridad		A/R	C
política de seguridad	A	R	C
normativa de seguridad		A/R	C
procedimientos de seguridad		R	A
implantación de las medidas de seguridad	I	C	A/R
supervisión de las medidas de seguridad	I	A	R
estado de seguridad del sistema	I	A	R

planes de mejora de la seguridad		A/R	C
planes de concienciación y formación		A/R	C
planes de continuidad		R	A
suspensión temporal del servicio	A	C	R
seguridad en el ciclo de vida		C	A/R

7.3.- PROCEDIMIENTOS DE DESIGNACIÓN

Los cargos anteriores, se revisarán cada 2 años, o cuando se considere oportuno por parte de la dirección de la empresa.

7.4.- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión de la dirección de DIGITAL VALUE S.L. la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la dirección y difundida a través de la intranet y la web para que la conozcan todas las partes afectadas.

7.5.- RESOLUCIÓN DE CONFLICTOS

Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité de Seguridad de la organización, y prevalecerá en todo caso el criterio de la Dirección.

8.- DATOS DE CARÁCTER PERSONAL

DIGITAL VALUE S.L. trata datos de carácter personal. El Documento de Seguridad que se puede encontrar en la intranet en la sección de Documentos > Gestión Seguridad recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de DIGITAL VALUE S.L. se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

9.- GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

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

10.- DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

10.1. -ESTRUCTURACIÓN

La información está estructurada atendiendo a la clasificación de los sistemas principales de los que consta la empresa. De esta forma encontraremos los siguientes manuales de operación:

- Manual de del Sistema de Gestión de la Seguridad de la Información.
- Manual de operación del Data Center.
- Manual de operación de la Plataforma de Alojamiento Web
- Manual de operación de la Plataforma de Correo Electrónico
- Manual de Calidad y Seguridad en el Desarrollo de Aplicaciones
- Manual de operación de los Sistemas de Oficina

Cada uno de los documentos de seguridad de la información de DIGITAL VALUE S.L. deberá estar aprobado por el Responsable de Seguridad y el Responsable de Seguridad de la Información.

10.2.- GESTIÓN Y ACCESO

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. La normativa de seguridad estará disponible en la intranet https://intranet.digitalvalue.es.

Los documentos incorporan la clasificación de seguridad según la categorización siguiente:

PÚBLICO	Puede darse difusión a esta información a todos los interesados, incluyendo personal y clientes, sin ninguna limitación.
INTERNO	Documento CONFIDENCIAL. Disponible únicamente para empleados de la compañía y tiene restringida la difusión fuera del grupo.
RESERVADO	Documento CONFIDENCIAL con grupo de usuarios restringido por rol o categoría y tiene restringida la difusión fuera del grupo.
SECRETO	Solo disponible para las personas autorizadas sin derecho de difusión ni de desvelación a terceros.

11.- OBLIGACIONES DEL PERSONAL

Todos los miembros de DIGITAL VALUE S.L. tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Responsable del Sistema disponer los medios necesarios para que la información llegue a los afectados.

Las actuaciones del personal estarán supervisadas por el responsable del sistema pertinente atendiendo al apartado *6.2 Roles y Responsabilidades* de la presente Política de Seguridad.

Todos los miembros de DIGITAL VALUE S.L. atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de DIGITAL VALUE S.L., en particular a los de nueva incorporación. El Responsable del Sistema impartirá estas sesiones de concienciación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Cada usuario poseerá un identificador generado atendiendo a los requisitos especificados en el documento *[op.acc.1] Identificación* con el que deberá acceder al sistema mediante identificador y contraseña. De esta forma se incide en la dimensión de trazabilidad de los sistemas.

Las funciones y obligaciones concretas del personal se pueden encontrar en el Documento de Gestión de la Seguridad disponible en la intranet.

12.- TERCERAS PARTES

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

Cuando DIGITAL VALUE S.L. utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe 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 esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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

13.- ADQUISICIÓN DE PRODUCTOS

Se establece un proceso formal para la planificación y adquisición de nuevos componentes del sistema. En este proceso garantizará el cumplimiento de las conclusiones del análisis de riesgos, la compatibilidad con la arquitectura de seguridad, y que se contemplen las necesidades técnicas de formación y financiación.

Para ello se ha dispuesto en la Intranet un apartado de Registro para identificar las adquisiciones, hacer un seguimiento de las mismas y revisar y confirmar las condiciones enunciadas antes de su incorporación dentro de la estructura operativa de la empresa. Para ello se requerirá de la aprobación expresa por parte de la Dirección.

Los detalles de este proceso se han incorporado al manual de procedimiento Operativos que está disponible en la Intranet.

14. REGISTRO DE ACTIVIDAD

Todas las actividades y actuaciones de los usuarios en los sistemas serán registradas de forma que se registrará quien realiza la actividad, cuando la realiza y sobre qué información. Se incluirá la actividad de los usuarios y especialmente, la de los operadores y administradores, las actuaciones realizadas con éxito y los intentos fallidos.

La determinación de las actividades que se registrarán y los niveles de detalle se adapta al análisis de riesgos realizado según los niveles.

Para ello los equipos y servidores han sido configurados para registrar automáticamente esta información. Todos los empleados han recibido y confirmado el documento “Aceptación y Recepción” donde han sido informados y obligados al mantenimiento y preservación de esta información, y al mantenimiento de los registros manuales que les sean requeridos.

15. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Todo elemento físico o lógico requerirán autorización formal previa a su instalación en el sistema, tal como se ha descrito en el punto 12. En este proceso se tendrán en cuenta las especificaciones del fabricante, las vulnerabilidades y las actualizaciones que les afecten.

De la misma manera se atenderá en todo momento el estado de seguridad de los sistemas en operación, en relación a las vulnerabilidades y a las actualizaciones, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.
Para ello se desarrollará la política de mantenimiento de equipos, sistemas y aplicaciones que está desarrollada en el Manual de Operaciones, y se han dispuesto los Registros correspondientes para anotar las revisiones de seguridad regulares realizadas y las revisiones extraordinarias que hayan sido requeridas a los avisos, alarmas y alertas recibidos.

La gestión de estas actuaciones, tanto las regulares como las extraordinarias, se registran detalladamente en la Intranet.

16. PROFESIONALIDAD

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. Instalación, mantenimiento, gestión de incidencias y desmantelamiento.

La empresa facilitará a su personal la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la empresa.

La empresa exigirá a sus proveedores y terceros que les prestan servicios técnicos y de seguridad, que sus profesionales cuenten con la capacitación y profesionalidad y unos niveles idóneos de gestión y madurez en los servicios prestados.

17. SEGURIDAD POR DEFECTO

Todos los sistemas que proporciona esta empresa, y aquellos que se utilizan en la producción de los servicios y productos, han sido diseñados y configurados para garantizar la seguridad por defecto.

- Proporcionan la funcionalidad mínima requerida para alcanzar sus objetivos
- Incorpora las funciones necesarias de administración, operación y registro de actividad, y solo son accesibles por las personas, y desde los emplazamientos y sistemas autorizados, con posibilidad de exigir restricciones de horarios de acceso.
- Todos los sistemas de explotación pueden desactivar o eliminar las funciones que no sean de interés, innecesarias, o inadecuadas.
- El uso ordinario será siempre sencillo y seguro, de toda utilización insegura requerirá siempre de un acto consciente por parte del usuario.

CLASIFICACIÓN DE LA INFORMACIÓN

Nombre del fichero	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
Tipo de documento	**PROCEDIMIENTO**
Clasificación	PÚBLICO
Creado	PABLO BARRACHINA SANTANA
Aprobado	PABLO BARRACHINA TORTAJADA

Fecha	Versión	Cambios realizados	Autor o responsable
16/07/2022	1.0	Versión inicial	Pablo Barrachina Santana
01/03/2024	3.0	Actualización al RD 311/2022	Pablo Barrachina Santana
