POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (ENS)

KEYTRON S.A.

Índice

PROCESO: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (ENS) KEYTRON S.A..	**PROPIETARIO:** GERENCIA
MISIÓN: Política de seguridad de la información en el marco del ESQUEMA NACIONAL DE SEGURIDAD	**NORMA APLICACIÓN:** RD 311/2022, del 3 de mayo RD 3/2010 (ENS) RD 951/2015 UNE-ISO/IEC 27001:2013

BREVE DESCRIPCIÓN DE LA ORGANIZACIÓN:

Desde su constitución en el año 1988, KEYTRON S.A. se ha especializado en ofrecer a sus clientes soluciones innovadoras, consolidándose durante este tiempo como una empresa de referencia en servicios TIC.

Nuestro principal objetivo es la satisfacción de nuestros clientes, para lo que ponemos todos los medios necesarios y aportamos soluciones eficientes, innovadoras y de calidad en cada caso.

A lo largo de todos estos años hemos demostrado que existe otra forma de hacer las cosas con éxito y optimizando recursos, por ello actualmente contamos con numerosos clientes de todos los sectores y tamaños que avalan nuestra gestión.

Empresa de capital 100% español.

Más de 10 años de experiencia en servicios TIC.

Foco en servicios sobre infraestructura IT.

Servicios prestados a Administraciones Públicas que se ven afectados dentro del alcance fijado para el ENS

Cobertura a nivel nacional.

Actividades desarrolladas por KEYTRON S.A. en el marco del ENS:

- Soporte y Gestión de Infraestructuras
- Servicios Gestionados
- Infraestructura IT
- Servicios Cloud
- Proyectos Transformación IT

ALCANCE:

Servicios de soporte y mantenimiento de infraestructura hardware, software y otros servicios asociados (instalaciones, consultoría, proyectos, asistencias técnicas).

CENTROS Y DIRECCIONES:

- San José Artesano 12, 28108 Alcobendas

CLIENTES EXTERNOS:

Clientes de tipología pública.

PROVEEDORES:

Fabricantes y distribuidores acorde con las actividades de la empresa:

Están identificados en el fichero “BD_Proveedores”

PROCESOS EXTERNALIZADOS:

10% externalización. Instalación redes.

CONTEXTO INTERNO.

Plantilla

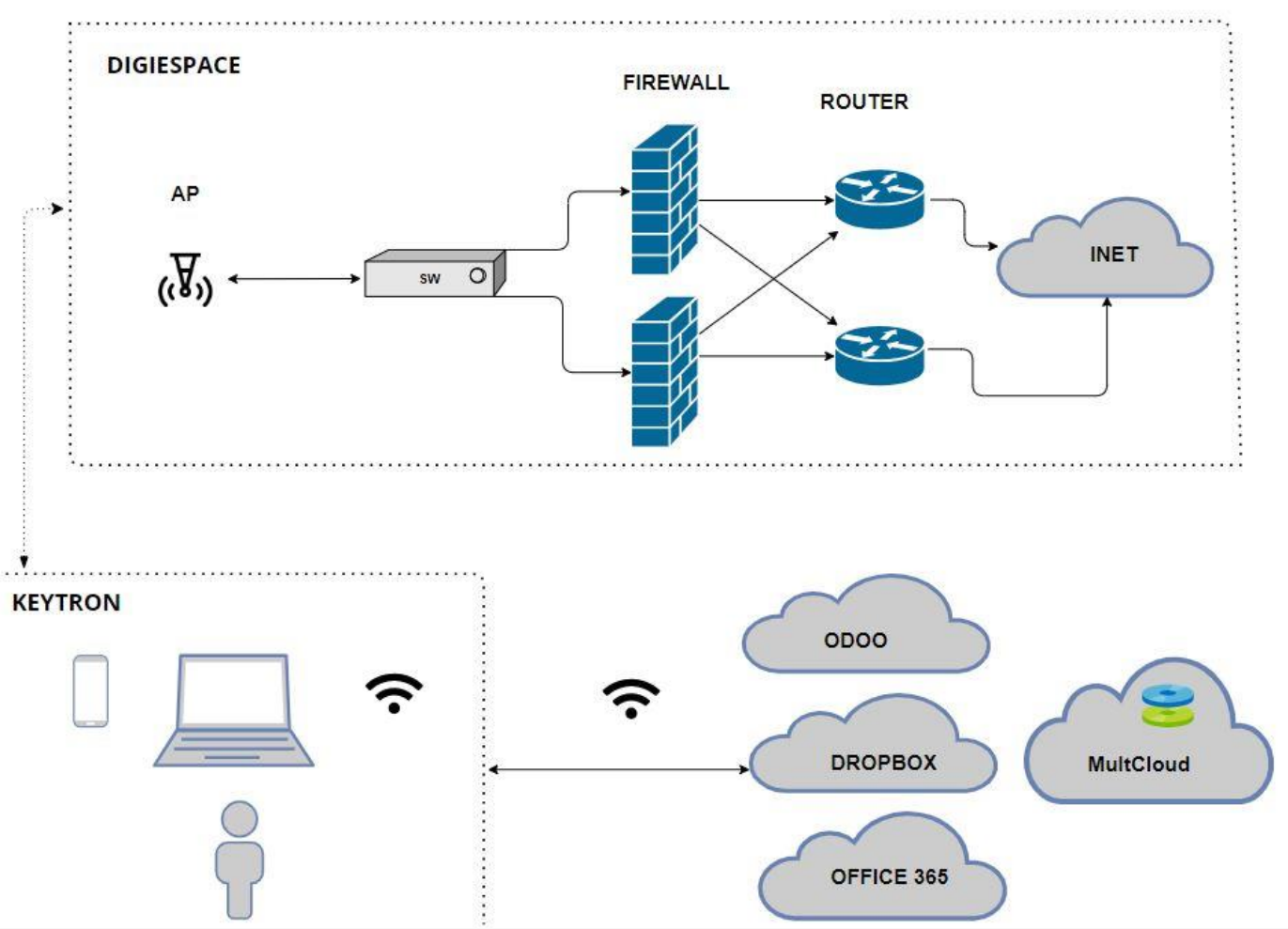
La plantilla de KEYTRON S.A. consta de una media de 18 empleados.

Instalaciones

KEYTRON S.A. se encuentra en una nave en la calle Guzmán el Bueno 16 de Alcobendas.

En este edificio es Digiespace Work S.L. quien gestiona los mantenimientos correspondientes de la infraestructura.

Mapa/Topología de red



LEGISLACIÓN/REGLAMENTACIÓN APLICABLE PRESTACIÓN DEL SERVICIO:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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.
- 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.

- L.O. 3/2018, de 5 de diciembre de Protección de Datos Personales y Garantías de los Derechos Digitales.
- Real Decreto 513/2017. Reglamento de instalaciones de protección contra incendios.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

1. Introducción

KEYTRON S.A. es una empresa que presta servicios de soporte y mantenimiento de infraestructura hardware, software y otros servicios asociados prestados a Administraciones y organismos públicos.

KEYTRON S.A. tiene personalidad jurídica propia y plena capacidad de obrar para administrar, adquirir, contratar, asumir obligaciones, así como renunciar y ejercer libremente toda clase de derechos y acciones ante las Administraciones públicas.

En el nuevo marco de la administración electrónica, y para su correcto desarrollo **KEYTRON S.A.** presta servicios a las propias administraciones y organismos públicos con los que colabora, y para ello, proporciona las mayores garantías para el correcto uso de las tecnologías por parte de las Administraciones Públicas.

KEYTRON S.A. establece objetivos de seguridad de la información encaminados a proteger con las mayores garantías, la integridad, la confidencialidad, la disponibilidad, la trazabilidad y la autenticidad de la información objeto de tratamiento dentro de sus competencias.

Para garantizar una apropiada seguridad de la información, **KEYTRON S.A.** aplicará las más adecuadas medidas de seguridad, en todos los Departamentos reforzando la prevención, detección y respuesta de incidentes de seguridad.

Los sistemas de información y comunicación de **KEYTRON S.A.** deben estar protegidos contra potenciales amenazas que puedan poner en peligro la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información. A tal fin, adoptarán una estrategia de seguridad de la información que permita cumplir con los requisitos establecidos por el Esquema Nacional de Seguridad; aplicar un sistema de mejora continua, supervisar y garantizar unos adecuados niveles de servicios; seguir y analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes de seguridad con el fin de garantizar la continuidad de los servicios.

Dentro del enfoque de la seguridad de la información como parte integral de los servicios prestados por **KEYTRON S.A.** y de su funcionamiento interno, tiene una especial importancia la protección de datos personales, por lo que muchas de las medidas implantadas estarán encaminadas a proteger proactivamente dichos datos, velando por el cumplimiento de lo dispuesto en la legislación vigente en materia de protección de datos personales dentro del marco normativo europeo y español.

2. Alcance

Esta política es aplicable, sin excepciones a:

- Todos los sistemas de información y comunicación.
- Todos los Departamentos.
- Todo el personal de KEYTRON S.A.
- Todo el personal externo que preste servicios a KEYTRON S.A.
- Todo el personal, electo o profesional perteneciente a las entidades delegantes que puedan acceder a los sistemas de información de KEYTRON S.A.

3. Misión

Los objetivos de servicio de KEYTRON S.A. son los siguientes:

I. Colaborar con las entidades locales y demás entidades públicas en la aplicación de sus tributos y demás ingresos de derecho público.
II. Ofrecer los mejores servicios de información y asistencia a los ciudadanos para el cumplimento de sus obligaciones y el ejercicio de sus derechos
III. Integrar el sistema de gestión de protección de datos adaptado al RGPD en el ENS.
IV. Reforzar la cultura de la organización en materia de seguridad de la información y protección de datos.
V. Situar a KEYTRON S.A. en el cuadrante de las entidades más avanzadas en materia de seguridad de la información en el ámbito de los servicios prestados a las Administraciones Públicas.
VI. Garantizar la disponibilidad de los servicios.
VII. Velar por los derechos y libertades de los ciudadanos y demás interesados en materia de protección de datos personales.

4. Marco legal y regulatorio aplicable

La legislación aplicable a KEYTRON S.A. en el marco de la seguridad de la información es la siguiente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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.
- 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.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de Acceso electrónico de los ciudadanos a los Servicios Públicos.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de

carácter personal, vigente en aquellos artículos que no contradigan, se opongan o resulten incompatibles con lo dispuesto en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre.

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

5. Organización de la seguridad

5.1 Comité de seguridad

El Comité de Seguridad KEYTRON S.A. está compuesto por el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

El Comité tiene las siguientes funciones:

a) Promover la seguridad de los activos de información de KEYTRON S.A.
b) Validar, la documentación de seguridad elaborada por el responsable de seguridad
c) Proponer la aprobación de la clasificación de la información, conforme a lo que se indica más adelante.
d) Valorar y proponer la aprobación de toda la documentación de seguridad.
e) Diseñar la estructura de la documentación de seguridad.
f) Vigilar el cumplimiento de las obligaciones del responsable del registro de actividades, conforme las regula la normativa de protección de datos de carácter personal.
g) Difundir entre el personal al que se refiere el ítem 2 del presente documento, el conocimiento de las obligaciones que le atañen y las consecuencias en que pudiera incurrir en caso de incumplimiento.

El detalle de las funciones del comité de seguridad se encuentra en "**Roles_Competencias_Funciones".**

5.2 Responsable de la información y del servicio

El responsable de la información es habitualmente una persona que ocupa un alto cargo en la dirección de la organización. Este cargo tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. El responsable de la información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

El responsable de la información será designado por la dirección de KEYTRON S.A. y tiene como responsabilidad la ejecución de todas las medidas de seguridad adecuadas para KEYTRON S.A., incluida la elaboración de la documentación de seguridad. Este cargo se irá renovando

automáticamente hasta que la Dirección General anuncie la sustitución de la persona que ocupa el cargo.

El responsable de la información dispone de la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información.

Determinar los niveles de seguridad de los servicios.

La Dirección KEYTRON S.A. garantizará que el responsable de la información participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad de la información y a la protección de datos personales.

La Dirección de KEYTRON S.A. respaldará al responsable de la información en el desempeño de las funciones mencionadas en el artículo 39 del RGPD, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

La Dirección de KEYTRON S.A. garantizará que el responsable de la información no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. El responsable de la información rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

Las personas interesadas podrán ponerse en contacto con el responsable de la información por lo que respecta a todas las cuestiones relativas a la seguridad de la información y a la protección de datos personales.

El responsable de la información estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

El responsable de la información podrá desempeñar otras funciones y cometidos. La Dirección General garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja (a veces se dice que 'se heredan los requisitos'), y suele añadir requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

El responsable de la información tendrá como mínimo las siguientes funciones:

a) Informar y asesorar a la Dirección General y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del ENS y de otras disposiciones aplicables en materia de seguridad de la información y de protección de datos, vigentes en España o en la Unión o de los Estados miembros;
b) Supervisar el cumplimiento de lo dispuesto en el ENS, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del

responsable en materia de seguridad de la información y protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la seguridad de la información y supervisar su aplicación de conformidad con lo dispuesto en el ENS;
d) Cooperar con las autoridades de control y los CERT.
e) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento de datos personales, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El detalle de las funciones del responsable se encuentra en "**Roles_Competencias_Funciones".**

El responsable de la información desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Aunque la aprobación formal de los niveles corresponde al responsable de la Información, se puede recabar una propuesta al responsable de la seguridad, así como también se escuchará la opinión del responsable del sistema.

5.3 Responsable del sistema

El responsable del sistema será designado por la dirección de KEYTRON S.A.. La persona designada figurará en la documentación de seguridad del sistema de información.

El responsable del sistema tendrá como mínimo las siguientes funciones:

a) Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
c) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
d) El responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de la Seguridad, antes de ser ejecutada.

El detalle de las funciones del responsable se encuentra en "**Roles_Competencias_Funciones".**

5.4 Responsable de seguridad

El responsable de seguridad será designado por la dirección de KEYTRON S.A. y tiene como responsabilidad la ejecución de todas las medidas de seguridad adecuadas para KEYTRON S.A., incluida la elaboración de la documentación de seguridad. Este cargo se irá renovando automáticamente hasta que la Dirección General anuncie la sustitución de la persona que ocupa el cargo.

Con independencia de la obligación genérica referida a la implantación, coordinación y control de las medidas de seguridad, se enumeran a continuación, a título enunciativo, las funciones mínimas concretas del responsable de seguridad:

a) Adoptar, con la mayor inmediatez, las medidas oportunas para subsanar cualquier anomalía que haya producido una incidencia e importar al Comité los impresos en que se hayan registrado las incidencias.
b) Cuando las incidencias hayan afectado a Datos personales, el responsable de Seguridad deberá comunicar inmediatamente la incidencia a la delegada de Protección de Datos.
c) Colaborar con el director y la delegada de Protección de Datos, en la comprobación de la correcta aplicación de los procedimientos de realización de copias de seguridad y recuperación de datos.
d) Verificar que en todo procedimiento de recuperación de datos que sea realizado por personal externo, se mantiene la más estricta confidencialidad sobre los datos de carácter personal objeto de tratamiento.
e) Verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
f) Custodiar y actualizar la relación de usuarios con acceso a los sistemas de información o que intervienen en los tratamientos de datos de carácter personal.
g) Supervisar con la responsable de Protección de Datos, el nivel de intervención, por los usuarios dados de alta, en las diferentes fases del ciclo de vida de los tratamientos de datos de carácter personal.
h) Asignar a los nuevos usuarios el correspondiente código de usuario y una contraseña, dándoles las instrucciones para que cambien la contraseña asignada en un plazo no superior a veinticuatro horas, de tal forma que la contraseña pase a ser del exclusivo conocimiento del usuario.
i) Borrar los identificadores de usuario y contraseñas cuando un usuario sea dado de baja.
j) Autorizar expresamente a la persona que entregue para su salida, o reciba de terceros, soportes informáticos que contengan datos de carácter personal. La autorización la realizará de forma específica para cada recepción o entrega, mediante firma en el impreso correspondiente, o de forma genérica, también mediante autorización escrita.
k) Conservar los impresos cumplimentados de entradas y salidas de soportes.

l) Controlar los mecanismos establecidos para el registro de accesos, los cuales no podrán ser desactivados en ningún caso.
m) Establecer y comprobar todos los procedimientos y estándares necesarios para la correcta aplicación de la normativa de seguridad.

El detalle de las funciones del responsable se encuentra en "**Roles_Competencias_Funciones".**

5.5 Usuarios

Los usuarios / personal técnico, acceden a las aplicaciones con el perfil suficiente para desempeñar sus funciones profesionales, debido a la función asignada o del puesto de trabajo que despeñan y de la unidad administrativa en la que se encuadra.

El detalle de las funciones de los usuarios se encuentra en "**Roles_Competencias_Funciones".**

6. Concienciación y formación

Se desarrollarán actuaciones de concienciación y formación. El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de la organización y a todas las actividades, de acuerdo con el principio de Seguridad Integral recogido en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Se desarrollarán actuaciones de concienciación y formación. El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de la organización y a todas las actividades, de acuerdo con el principio de Seguridad Integral recogido en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

7. Herramientas de seguridad

7.1 Clasificación de la documentación

La documentación de seguridad se clasifica en cuanto a su contenido del siguiente modo:

a) **Política de seguridad**: El presente documento, que establece las directrices generales de la seguridad en KEYTRON S.A. al más alto nivel.
b) **Normativa de seguridad**: El documento que establece la obligatoriedad de la documentación de seguridad.
c) **Políticas particulares**: Documentación que establece directrices de actuación en áreas determinadas.
d) **Procedimientos:** Documentos que establecen maneras concretas de actuación.
e) **Registros**: Documentos que reflejan los resultados de los procedimientos.
f) **Inventarios:** Relación de ítems en un momento determinado.
g) **Documentos para la gestión de riesgos**: Análisis de impacto y plan de continuidad.

h) **Otra documentación**: Cualquier otra documentación relevante a la seguridad de la información procesada por KEYTRON S.A.

Dentro de esta documentación se incluye toda la documentación relevante al cumplimiento de la Legislación vigente en materia de protección de datos personales.

7.2 Procedimiento para la clasificación

La clasificación la realiza el responsable de seguridad, bajo la supervisión del comité de KEYTRON S.A.

7.3 Generación y aprobación de la documentación

La documentación la genera el responsable de seguridad, o personal bajo su dirección, la propuesta la realiza el comité y la aprueba la dirección de KEYTRON S.A.

7.4 Acceso a la documentación

El acceso a esta documentación se autoriza por el responsable de seguridad, previa deliberación en el comité. A cada usuario sólo se le conceden los privilegios mínimos para cumplir con estas obligaciones.

La difusión de determinada documentación está regulada en los correspondientes procedimientos de difusión.

7.5 Revisión de la documentación de seguridad

La revisión de la documentación de seguridad se realiza conforme a los procedimientos que se establezcan.

7.6 Protección de las instalaciones

La protección de las instalaciones se encuentra descrita en el Procedimiento de Gestión de la Seguridad Física y del Entorno.

7.7 Adquisición de productos

Antes de la adquisición de cualquier producto de seguridad de la información aplicable al alcance incluido dentro del ENS, se seguirán las pautas descritas en la Guía del CCN 105 Versión febrero 2021.

7.8 Seguridad por defecto

Antes de realizar ningún tipo de modificación de políticas, procedimientos o usos de nuevas herramientas aplicables a los servicios que se prestan a las Administraciones y organismos públicos en el marco del alcance del ENS, se tendrán en cuenta todos los aspectos de seguridad de la información requeridos por el ENS, la Norma ISO 27001, otra legislación aplicable que resulte de aplicación, así como cualquier otro requisito de seguridad de la información requerido por cualquier Administración u organismo público que contrate cualquiera de los servicios enmarcados dentro del alcance del ENS.

7.9 Política de autenticación y acceso al sistema

7.9.1 Formación de las contraseñas

Se evitarán nombres comunes, o cualquier otra combinación que pueda identificar al usuario (fecha nacimiento, matrículas de vehículos, etc.).
Recomendaciones para uso de contraseñas:

a) Uso de reglas nemotécnicas: EuldlM “En un lugar de la Mancha”.
b) Sustituir números por letras. Ej. Sustituir la a por el 9, contr9señ9.
c) Tendrá una longitud mínima de 8 caracteres siempre que el sistema lo permita. Caso contrario se adoptará la longitud máxima posible.
d) Deberá cambiarse al menos una vez cada 180 días.
e) Existe habilitado un mecanismo para que no se pueda reutilizar las últimas 2 contraseñas que se usaron en el sistema.

El mecanismo de gestión de autenticadores no permite utilizar contraseñas que no cumplan esta política.

7.9.2 Validez de las contraseñas y otros métodos de autenticación

La cuenta del usuario no se habilita hasta que éste haya confirmado la recepción del modo de autenticación.

Las contraseñas deben cambiarse una vez al año.

7.9.3 Mensajes previos al acceso y mensajes de error en el acceso

Los sistemas, deben ser configurados de forma que no revelen información del sistema antes de un acceso autorizado.
En particular, los diálogos de acceso no deben revelar información sobre el sistema al que se está accediendo.

Del mismo modo, los mensajes de error en el acceso deben revelar la información mínima necesaria.

7.9.4 Reacción del sistema ante intentos repetidos de acceso sin éxito

El número máximo de intentos fallidos de acceso es de cinco. Tras el quinto acceso sin éxito al sistema o a una aplicación determinado, el usuario queda bloqueado.

Un bloqueo de usuario es una incidencia que debe gestionarse conforme al procedimiento de gestión de incidencias.

El sistema almacena un registro con los accesos exitosos y los fallidos, tal y como se establece en la política de retención de registros de actividad.

7.9.5 Política de renovación de la autenticación del usuario

El procedimiento de gestión de accesos establece los puntos en los que el sistema requerirá una renovación de la autenticación del usuario.

7.9.6 Política de accesos remotos

Los accesos desde fuera de las propias instalaciones de KEYTRON S.A. deben cumplir los requisitos establecidos.

8. Procedimiento de coordinación y resolución de conflictos y reclamaciones

En caso de conflicto entre los distintos perfiles de puesto integrados en el comité de seguridad, prevalecerán las instrucciones facilitadas por la dirección General y, en su defecto por el responsable de Seguridad de la Información.

Para las reclamaciones, se encuentra vigente y resulta de aplicación el procedimiento de gestión relaciones con el negocio.
Las reclamaciones quedan registradas en la base de datos de incidencias donde se hace un seguimiento exhaustivo de las mismas.

9. Integridad y actualización del sistema

Cualquier elemento físico o lógico requiere la autorización del responsable de Seguridad de la Información para poder proceder a su instalación en los sistemas de información de KEYTRON S.A.

Se realizan test periódicos de vulnerabilidades técnicas para comprobar el estado de la seguridad de los sistemas de información de KEYTRON S.A.

10. Prevención ante otros sistemas de interconexión interconectados

KEYTRON S.A. no cuenta con sistemas de interconexión interconectados en los servicios que presta a los Organismos y Administraciones Públicas en el marco del alcance del ENS.
NOTA: Se tiene en cuenta la Guía CCN-STIC 811 de Interconexión en el ENS.

11. Entrada en vigor

Esta Política de Seguridad de la Información es efectiva desde el día siguiente de su aprobación y hasta que no sea reemplazada por otra versión posterior.

34794880C EVA MARIA PRIETO (R: A78879285)

Firmado digitalmente por: 34794880C EVA MARIA PRIETO (R: A78879285)
ND: CN = 34794880C EVA MARIA PRIETO (R: A78879285) C = ES O = KEYTRON SA
Fecha: 2023.10.18 17:09:25 + 01'00'