POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fecha de aprobación 8 de agosto de 2020

INTRODUCCIÓN

WURTH S.L. ha considerado la necesidad de gestionar la seguridad como un todo completo, transversal en la entidad y en cada proceso interno, como una cuestión estratégica de la organización.

La implementación de un sistema de gestión de la seguridad de la información, está condicionada a las necesidades de negocio y a las líneas marcadas por los objetivos organizacionales, entre los que se encuentran actualmente, los objetivos de seguridad de la organización. Todos los procesos internos y externos, quedan adscritos y afectos, a la presente política de seguridad, o cuantas políticas transversales se desarrollen para dar cumplimiento a la misma.

La seguridad, por tanto, debe ser entendida como el conjunto de principios básicos y requisitos mínimos requeridos para una protección adecuada de la información tratada y los servicios prestados a los terceros.

Nuestra organización ya ha venido dando pasos en este sentido, y ha considerado prioritario establecer los objetivos de seguridad con plena alineación con los objetivos de negocio que culminará en un sistema de gestión conforme a los requisitos establecidos en el Real Decreto 3/2010 –en su versión consolidada por Real Decreto 925/2015-, y que culminará con la certificación en esta línea y en un sistema de gestión de seguridad de la información.

Por defecto, la Dirección ha considerado que la organización es la responsable de los activos de información y de los recursos de su propiedad, y asume que las tareas relacionadas con la seguridad de la información son una parte fundamental para el desarrollo de negocio.

Se mantendrán las tres dimensiones clásicas de seguridad, integrándose además las dimensiones referenciadas en el Real Decreto 3/2010: confidencialidad, integridad y disponibilidad, así como dimensiones de autenticidad y trazabilidad.

La organización considera que la seguridad de la información debe evolucionar continuamente para adecuarse a los requerimientos de negocio, sin impactar injustificadamente en el mismo y teniendo en cuenta la adecuada relación entre costes y beneficios.

Para soportar esta política, se establecerán políticas de seguridad, normas y procedimientos detallados, los cuales serán publicados y comunicados a todos los usuarios, terceros y socios de negocio de WURTH S.L. cuando los mismos se vean afectados. La presente Política será accesible para las partes internas y externas afectadas.

Estándar de seguridad de la información

La Dirección, ha considerado implantar un estándar de seguridad. Se considerarán todos los elementos de seguridad necesarios, y específicamente el Real Decreto 3/2010 (en su versión consolidada por Real Decreto 951/2015).

En base a este estándar, se ha impuesto un sistema, con los requisitos propios de un sistema de gestión de seguridad de la información, considerando las particularidades del negocio, de la organización y del cliente tipo.

La organización somete sus sistemas a los controles establecidos en su Política de Seguridad, y en su caso, cuando sea preciso, se incorporarán nuevos controles o se complementaran los mismos.

La organización puede considerar la necesidad de someterse a una certificación de un tercero externo independiente, que permita acreditar la alineación el sistema de gestión implantado a la norma, según descripción de la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad (ENS). La organización considerará otras normas de uso no obligatorio, pero de referencia, y específicamente la serie de Guías 800 publicadas por el Centro Criptológico Nacional CCN-CERT.

La organización debe cerciorarse que la seguridad es una parte integral de cada etapa del ciclo de vida del sistema y de la información, desde el diseño de un producto o un servicio hasta su retirada. Incluyendo las diferentes fases de desarrollo o adquisición y la propia producción o explotación. El sistema deberá estar diseñado para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad.

ESTRATEGIA CORPORATIVA

Se implanta una estrategia corporativa para garantizar la seguridad del sistema y el adecuado servicio prestado, lo que implica necesariamente que todos los recursos deben disponer y aplicar las medidas mínimas de seguridad exigidas, y en concreto las que sean de aplicación de las contenidas en el Anexo II 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.

OBJETIVO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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 para detectar cualquier incidente y reaccionando con urgencia a los incidentes para recuperarse lo antes posible y minimizar el impacto.

Este objetivo de la política de la seguridad de la información se complementa por la protección de los activos que soportan el sistema de información de la organización y los procesos internos, implicados en los servicios declarados en este documento, quedando afectadas las tres dimensiones de seguridad –confidencialidad, integridad y disponibilidad-, y cuando fuera preciso, incorporando otras dimensiones –autenticidad y trazabilidad- (por requerimiento legal), quedando alineada plenamente con los objetivos de negocio e integrándose en la estrategia de la organización.

Por último, dicho objetivo deberá alinearse el requerimiento legal del 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 esos datos – Reglamento General de Protección de Datos (RGPD), por lo que se considera a todos los efectos, este documento como el documento de alto nivel que declara la Privacidad como integrada en la Estrategia de Seguridad corporativa y en el Objetivo General de Seguridad.

Servicios - Línea de negocio

WURTH SL basa su línea de negocio en la fabricación de soluciones informáticas (aplicaciones) y prestación de servicios relacionados con los mismos, en el sector de la Administración Local. Para llevar a cabo sus objetivos, la empresa se divide en cuatro áreas: dirección, administración, desarrollo de producto y soporte/asesoramiento. Los productos informáticos están diseñados para dar solución a la gestión municipal (Área económica, RRHH, Área de Estadística y Área Tributaría-Recaudación). A cada producto informático le corresponde un servicio de mantenimiento anual correctivo, evolutivo y legislativo, que es prestado por las áreas de Desarrollo y Soporte/Asesoramiento.

Objetivos particulares de seguridad de la información

Los objetivos de seguridad de la información definidos por WURTH S.L., han sido desarrollados y aprobados por la Dirección, considerando los requerimientos identificados de las partes interesadas (internas y externas), la gestión de los riesgos y para cumplir con los requisitos de seguridad establecidos por la organización.

La organización ha establecido como objetivos clave de la seguridad de la información, los siguientes:

- Mantener el pleno cumplimiento legal alineando los procesos y los servicios, a la normativa vigente en cada momento, y que afecta de manera indirecta o directa, al perfil de cliente (privado o administración pública), a la información implicada (pública, restringida o secreta) o en general a la seguridad de la información. Especial referencia al declarado Reglamento Europeo y en obviamente, al Real Decreto 3/2010.
- Mantener una gestión adecuada del sistema de gestión de seguridad, mediante la eficiencia y eficacia de la seguridad, de acuerdo a los estándares de seguridad y las buenas prácticas del sector.
- Alinear el requisito legal y la gestión del sistema con la privacidad y la seguridad.
- Establecer y difundir los roles y responsabilidades relacionados con la Seguridad de la Información.
- Sensibilizar y concienciar de manera estable y permanente al usuario de la organización mediante el impulso de acciones por la Dirección y la ejemplificación de la misma, en las tareas de seguridad más críticas.

- Fomentar y mantener el buen nombre de la organización en relación a los servicios desarrollados, saber hacer y respuesta activa –reactiva y proactiva- ante incidentes de seguridad, manteniendo la imagen y reputación.
- Asegurar que los activos de la organización, sólo sean utilizados por usuarios autorizados en el ejercicio de sus funciones, según perfiles definidos o según asignaciones extraordinarias.
- Gestionar la implementación de un sistema de seguridad que proporcione ventajas competitivas en relación a otros agentes del sector, aprovechando la inercia competitiva que puede otorgar la gestión adecuada de la seguridad.
- Proteger la información interna y la relacionada con la prestación de los servicios / clientes, considerando las dimensiones de:
    - Confidencialidad: Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.
    - Integridad: Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
    - Disponibilidad: La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.

La organización podrá considerar otras dimensiones relacionadas con la seguridad, derivadas de requerimientos legales (o en su caso, de requerimientos de negocio), considerándose:

- Trazabilidad: Toda acción desarrollada en el sistema o sobre la información, puede ser imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.
- Autenticidad: Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a dudas.

Por defecto la organización mantendrá las tres primeras dimensiones de seguridad. Cuando sea preciso se añadirán los dos restantes.

PRINCIPIOS DE SEGURIDAD

La Dirección ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles Esquema Nacional de Seguridad.

El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por la Dirección. Existe un procedimiento de gestión documental, "Procedimiento de Gestión de la Documentación" (00-PR), que establece las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Todo el sistema está enmarcado por los siguientes principios:

Seguridad por defecto

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde localizaciones o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso.

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

Para mantener el proceso de seguridad integral, se realizará una calificación de la información-, conforme a los principios de protección frente a pérdidas, accesos indebidos, divulgación o uso indebido, deterioro de la información o pérdida de disponibilidad. La calificación conllevará necesariamente una política de etiquetado y manipulación.

Se deberá conocer en todo momento el estado de seguridad del sistema o de sus componentes, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les puedan afectar.

Seguridad basada en el liderazgo y en la organización

La seguridad deberá comprometer a todos los miembros de la organización, en base a sus diferentes roles, considerando diferentes responsabilidades.

La Dirección será quien lidere la organización y promueva la cultura de seguridad, asignando los roles requeridos y potenciando la transversalidad de la seguridad en cada proceso desarrollado o servicio a terceros.

La seguridad del sistema será revisada de conformidad a los requisitos, la política y los procedimientos aprobados por la Dirección. Las revisiones serán por parte de la Dirección y por revisiones internas o auditorias del sistema. Específicamente la entidad y el sistema se podrán someter a procesos de certificación externos, conforme a lo establecido por el Esquema Nacional de Seguridad y cualquier otro estándar de seguridad que le pudiera interesar.

Organización de la Seguridad

Se establece una estructura organizativa en la organización, donde se establecerán roles específicos, pero siempre considerando el principio de separación de funciones. Se designarán a las personas que ocuparán los roles, por periodos anuales, pudiendo ser renovados automáticamente cuando transcurra el citado plazo y la Dirección no establezca una nueva persona para ocupar el cargo.

Mediante anexo a la presente Política se nombrarán y aceptarán los cargos. Como anexo se incorpora también las tareas preceptivas de cada rol establecido:

A) Comité de Seguridad:

Será el órgano encargado de desarrollar las directrices y estrategia de seguridad. Estará formado por el Director, que actuará como Presidente, el Responsable de Seguridad y el Responsable del Sistema.

El Comité, puede recabar regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.

Este Comité será convocado cuando, aparezcan incidentes de seguridad graves y específicamente cuando surjan nuevas necesidades de seguridad.

El Comité se reunirá al menos una vez al año de manera ordinaria y extraordinariamente cada vez que sea necesario, con una convocatoria previa, de al menos 3 días laborales, efectuada por la Dirección, mediante correo electrónico. El Comité podrá ser requerido por el Responsable de Seguridad, en cuyo caso la Dirección deberá convocarlo en un periodo máximo de 15 días laborales.

B) Responsable del Sistema:

Será considerado el operador del sistema. Podrá incluso paralizar o dar suspensión al acceso a la información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

C) Responsable de Seguridad:

Gestionará la seguridad entendida como objetivo transversal u embebido en la estrategia corporativa. Mantendrá y verificará los requisitos de seguridad del sistema y de la información que se pudiera gestionar.

D) Administrador del sistema:

Realizará funciones de administrador del sistema y aplicará medidas junto con el Responsable del Seguridad y el Responsable de Sistema

Seguridad basada en procedimientos

La seguridad del sistema se documentará mediante procedimiento de operación que serán puestos a disposición de los usuarios implicados en el mismo. Los cambios serán gestionados, las capacidades del sistema serán medidas y controladas y los entornos estarán separados. Se desarrollarán procedimientos de protección del sistema, incluyendo procedimientos de copias y restauración, y cuantas vulnerabilidades pudieran tener el sistema. Estas podrán tener forma de procedimiento general o especificaciones técnicas acordes a los operadores del sistema y de la seguridad.

Se documentarán los acuerdos con proveedores y colaboradores formando parte del sistema. La cadena de suministro será controlada con relación a los requisitos de seguridad, la prestación de servicios o los cambios de suministradores.

Las redes serán gestionadas, incluyendo cuando sea necesario, el cifrado o el control de comunicaciones.

Seguridad gestionada en base al riesgo

La gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado en el seno de la organización, bajo el liderazgo de la Dirección.

La gestión de riesgos se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema de información y la organización, basándose en una metodología detallada y documentada que permita la repetición de la medición y análisis.

Seguridad considerando incidentes

El proceso de gestión de incidentes, incluirá la detección y notificación de los incidentes de seguridad, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas –especialmente cuando afecta a terceros- y el registro de las actuaciones ejecutadas.

Los incidentes de seguridad permitirán la recopilación de evidencias, de manera que se podrá identificar, documentar la recogida, la adquisición y preservación de la información. Cuando estas evidencias afecten a acreditaciones de carácter legal, deberá contarse con el Delegado de Protección de Datos (DPD).

Continuidad de negocio

La continuidad formará parte del sistema de gestión, conforme a las necesidades de la organización y los controles establecidos. La organización considera el análisis de impacto y las consecuencias de la información que el mismo muestre.

Seguridad considerando la gestión de recursos

Todo el personal relacionado con el sistema y con la información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad, debiendo ser controlados y sus acciones supervisadas.

Cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se conozca, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

La responsabilidad será exigible mediante un procedimiento disciplinario, que al igual que pautas de seguridad, conocerá previamente el usuario. Este procedimiento estará alineado con la normativa laboral.

El usuario con acceso concedido al sistema, pueda o no desarrollar acciones, estará sometido a secreto y reserva, aun cuando finalice su relación con la organización. Ningún usuario accederá al sistema sin estar previamente informado de este extremo.

Seguridad de áreas y entorno

La organización prevendrá los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Las áreas podrán ser de control propio o derivada al propio prestador afectado

Seguridad como requisito legal.

La Dirección ha establecido como requerimiento de seguridad, el pleno cumplimiento de las obligaciones legales y contractuales, ligadas a la información. Los requisitos serán identificados y organizados, para su correcta gestión.

ALCANCE

La política de seguridad de la información, será de aplicación a toda la información del sistema con independencia del soporte o medio en el que se encuentre, tipología o categoría, a todo el personal de WURTH S.L. y también a terceros colaboradores, que accedan al sistema y/o presten servicios a la organización, así como a cualquier activo de información propiedad de la organización, o en régimen de uso y que afecte al sistema, considerándose en cualquier momento del ciclo de vida del sistema de seguridad, de manera que cuando el sistema se encuentre en fase de actualización, el activo no registrado se vea obligado por la política.

Con respecto a los sistemas de información afectados por el Real Decreto 3/2010, la organización ha decidido, que el ***alcance*** de su sistema de SGSI-ENS, será:

"Sistemas de Información propiedad de WURTH, S.L. relacionados con los procesos de desarrollo, instalación, mantenimiento y soporte técnico de las soluciones informáticas destinadas a la prestación de servicios a las Organizaciones públicas y privadas"

CUMPLIMIENTO

La Política de Seguridad de la Información tendrá vigencia desde la aprobación por el Comité de Seguridad y mientras no se apruebe una posterior, se mantendrá vigente. La Política de Seguridad será puesta en conocimiento de todos los afectados –internos y externos-.

La Política de Seguridad será alineada con las directrices de las leyes y regulaciones existentes. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente al Responsable del sistema.

Toda violación de la presente política o aquellas que la desarrollen, de las normas y procedimientos, será considerado por el procedimiento disciplinario, incluyéndose proveedores y colaboradores externos que serán tramitados por su procedimiento oportuno.

APROBACIÓN DE LA DIRECCIÓN

La Dirección de WURTH S.L., asume el compromiso de proveer todos los recursos y medios para la implementación la presente Políticas de su operatividad.

La Dirección demostrará su compromiso, mediante la revisión y aprobación de las Políticas y otras normas que desarrollaran el sistema, revisando los riesgos y aprobando el riesgo residual, considerando el informe de evaluación de impacto, participando en el Comité de Seguridad, promoviendo la cultura de seguridad, promoviendo la seguridad y especialmente, dotando de asignación efectiva a esta política mediante recursos y medios.