POLÍTICA DE SEGURIDAD

(ENS)

x	Copia Controlada
	Copia No Controlada
	Documentación obsoleta Fecha:……/……/……

	Aprobado por: Gerardo Cañibano Casarrubios Consejero delegado
	Firma: 50678234B GERARDO CAÑIBANO (R: A82921388) Firmado digitalmente por 50678234B GERARDO CAÑIBANO (R: A82921388) Fecha: 2021.09.03 18:47:01 +02'00'

Documentación pública: Este es un documento que contiene información que puede ser divulgada en cualquier medio sin que esto suponga ningún riesgo para la seguridad de la información.

Contenido

Documentación pública: Este es un documento que contiene información que puede ser divulgada en cualquier medio sin que esto suponga ningún riesgo para la seguridad de la información.

1. Introducción

WAIRBUT empresa dedicada a la Consultoría, Desarrollo de Soluciones/Servicios en el ámbito de IT, que inició su actividad en el 2001, pretende lograr una Mejora continua en la calidad, seguridad de la información, Gestión Ambiental y Gestión del servicio que presta. Por estas razones y para conseguir el máximo nivel de competitividad en el sector basada en la confianza y fidelización de nuestros clientes, desde la Dirección de WAIRBUT se impulsa la implementación, el mantenimiento y la mejora continua de su Sistema de Gestión basado en los requisitos de las normas de referencia UNE-EN ISO 9001 (Sistema de gestión de la calidad), UNE - ISO/IEC 20000-1 (Sistema de Gestión de Servicios), UNE-EN ISO 14001 (Sistemas de Gestión Ambiental) y UNE-ISO/IEC 27001 (Sistemas de Gestión de Seguridad de la Información), UNE 19601 (Sistema de Gestión de Compliance) y el Esquema Nacional de Seguridad.

2. Marco normativo

El marco normativo en materia de seguridad de la información en el que WAIRBUT desarrolla su actividad, esencialmente, es el siguiente:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
- 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.

- 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 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

3. Alcance

Aunque en WAIRBUT existe una política de seguridad implementada bajo la normativa EN-ISO/IEC 27001:2013 cuyo alcance afecta a todos los sistemas, trabajadores y proveedores que tengan relación con la empresa. **El alcance de la presente política son los sistemas de información que dan soporte a los servicios descritos para las administraciones y organismos públicos en el ámbito de las tecnologías de la información y de las comunicaciones:**

- **Diseño, desarrollo, mantenimiento y soporte de aplicaciones.**
- **Administración y mantenimiento de sistemas de información (infraestructura, hardware, sistemas operativos, base de datos, comunicaciones de datos y soporte al usuario de estos servicios).**

4. Principios y Directrices

WAIRBUT depende de los sistemas TIC[1] para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad o trazabilidad 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.

Según el Artículo 4 de los principios básicos del Esquema Nacional de seguridad, el objeto último de la seguridad de la información ***es asegurar que una organización pueda cumplir sus objetivos utilizando sistemas de información***. Para ello en las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

4.1 Seguridad integral

Para ello al menos se desarrollarán las siguientes actividades

[1] Tecnologías de Información y Comunicaciones.

a) Utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a Internet, el equipamiento informático y de comunicaciones.

b) Gestión de activos de información inventariados, categorizados y asociados a un responsable.

c) Mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de dichos sistemas.

h) Gestión de los incidentes de seguridad implantando mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad implantando mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.

4.2 Gestión de Riesgos

Sobre todos los sistemas sujetos a esta Política se 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

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada en el informe de Análisis y gestión de riesgos.

4.3 Prevención, reacción y recuperación

Para defenderse de las amenazas, los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema.

Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en las ofertas y en pliegos de licitación para proyectos TIC. Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

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

- Autorizar los sistemas antes de entrar en operación.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

4.4 Líneas de defensa

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 continuada para detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo establecido en el art. 8 y art. 9 del ENS.

Se establecerán Líneas de Defensa así como mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

4.5 Reevaluación periódica

Será misión del Comité de Seguridad la revisión y aprobación anual de esta Política de Seguridad de la Información. Esta Política será difundida para que la conozcan todas las partes afectadas.

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.

4.6 Función diferenciada

WAIRBUT y sus departamentos deben establecer como función diferenciada:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones con los Equipos de Respuesta a Emergencias (CERT[2])

[2] Computer Emergency Response Team: Conjunto de personas responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

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

5 Organización de la seguridad

La implantación de la Política de Seguridad en WAIRBUT requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado.

Como parte de la Política de Seguridad de la Información, los principales roles quedan identificados y detallados del modo siguiente:

- Responsable de Seguridad de la Información
- Responsable de Sistemas de la Información
- Responsable del Servicio de Asistencia Técnica
- Responsable de la Información

Estos puestos fueron designados por la dirección en la reunión mantenida el 18 de mayo de 2021 donde además de realizar los nombramientos se constituyó el Comité de Seguridad cuyas funciones son asumidas por el comité del Sistema de Gestión Integrado que ya existe en WAIRBUT.

Estas funciones y responsabilidades que se encuentran definidos en el procedimiento PCI-02 Roles Comité y su asignación nominal en el procedimiento PCI-02 Asignaciones, son las siguientes:

5.1 Funciones del responsable de Seguridad de la Información

- Asistencia al presidente del Comité de Seguridad en la elaboración del orden del día de las sesiones a celebrar.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de WAIRBUT.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
    - La estrategia de seguridad de la información definida por el Comité de Seguridad.
    - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de WAIRBUT
- Supervisar los incidentes de seguridad producidos en WAIRBUT.
- Difundir en WAIRBUT las normas y procedimientos contenidos en la Política de Seguridad de la Información, así como las funciones y obligaciones en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables en materia de protección de datos personales y de seguridad de la información.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de WAIRBUT.

5.2 Funciones del responsable de Sistemas de la Información

- Desarrollar, operar y mantener el Sistema de Información durante el ciclo de vida, 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.
- Seleccionar y establecer las funciones y obligaciones a los responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de WAIRBUT conforme a la estrategia de seguridad definida.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en WAIRBUT.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- 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.

5.3 Funciones del responsable del Servicio de Asistencia Técnica

- Tiene la facultad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad del servicio.

5.4 Funciones del responsable de la Información

- Establece los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación sobre protección de datos.

- Determina los niveles de seguridad de la información.

El nombramiento de estos roles se revisará cada 2 años o cuando el puesto quede vacante.

5.5 Difusión, actualización y revisión de la política de seguridad de la información

Será misión del Comité de Seguridad la revisión y aprobación anual de esta Política de Seguridad de la Información. Esta Política será difundida para que la conozcan todas las partes afectadas.

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.

5.6 Mecanismos de coordinación

WAIRBUT llevará a cabo esta actividad de monitorización sin utilizar sistemas o programas que pudieran atentar contra los derechos constitucionales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, manteniéndose en todo momento la privacidad de la información manejada, salvo que, por requerimiento legal e investigación sobre un uso ilegitimo o ilegal, sea necesario el acceso a dicha información, salvaguardando en todo momento los derechos fundamentales de los usuarios.

En los sistemas que se detecte un uso inadecuado o que no cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca.

El responsable de seguridad, con la colaboración de las restantes unidades de WAIRBUT, velará por el cumplimiento de la presente Normativa General e informará al comité de seguridad sobre los incumplimientos o deficiencias de seguridad observados, para que se tomen las medidas oportunas.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa.

Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino.

Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar al responsable de seguridad sobre usos prolongados e indebidos del servicio.

5.7 Gestión de Conflictos y medidas disciplinarias

En el supuesto de que un usuario no observe alguno de los preceptos señalados en la presente política, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.

WAIRBUT, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

- Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
- Monitorizará los accesos a la información contenida en sus sistemas.
- Auditará la seguridad de las credenciales y aplicaciones.
- Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

6. Datos de carácter personal

La Política de Protección de Datos y el Manual de Medidas de Seguridad al que tendrán acceso sólo las personas autorizadas, identifican los responsables de los tratamientos de datos personales, detallan estos tratamientos y exponen las medidas de seguridad correspondientes.

Todos los sistemas de información de WAIRBUT 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 Manual de Reglamento General de Protección de Datos (RGPD).

En aplicación del principio de responsabilidad proactiva establecido en el Reglamento General de Protección de Datos y la nueva LOPD, las actividades de tratamiento de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

Se aplicará, asimismo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

7. Obligaciones del personal

Todos los miembros de WAIRBUT tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de WAIRBUT atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de WAIRBUT, en particular a los de nueva incorporación.

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.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinares que procedan, sin prejuicio de las responsabilidades legales correspondientes.

8. Terceras partes

Cuando WAIRBUT 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 ataña a dichos servicios o información.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe 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.

9. Documentación de referencia

- PCI_ENS_PR_Normativa_Seguridad
- PCI-02 Roles Comité
- PCI-02 Asignaciones
- Esquema Nacional de Seguridad