POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN
ISBUT ESTUDIO 3 S.L

En vigor 12/05/2022

1 INTRODUCCIÓN

ISBUT 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 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 departamentos 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 todos los proyectos.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

1.1 Prevención

Los departamentos 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 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.

1.2 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.

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. La monitorización es especialmente relevante para evitar y/o minimizar incidentes.

1.3 Respuesta

Los departamentos 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 departamentos o en otros organismos.
- 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).

1.4 Recuperación

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.

2 ALCANCE

Esta política se aplica a todos los sistemas TIC de ISBUT y a todos los miembros de la organización, sin excepciones.

3 MISIÓN

La misión de Isbut es generar productos de calidad y dar un excelente servicio a nuestros clientes, para ello:

- Comprometidos con la **innovación**.
- Comprometidos con nuestros **clientes**, desde el descubrimiento conjunto de sus necesidades y la aportación honesta de las soluciones que mejor se adapten y respondan a ellas.
- Comprometidos con el **equipo humano**, plantilla, colaboradores y proveedores, con el que hacemos crecer, cada día, a las personas, a los profesionales, y a tu organización.
- Comprometidos con el **desarrollo sostenible**, apoyándonos en el triángulo del crecimiento económico, el equilibrio ecológico y el progreso social

4 MARCO NORMATIVO

La legislación de aplicación es la referente a tecnologías de la información y al acceso electrónico por parte de los ciudadanos. En particular aplican: 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) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El resto de leyes de referencia se encuentran identificadas en la pestaña correspondiente (“Legislación SI”) del documento “Listado de la Documentación en Vigor”

5 ORGANIZACIÓN DE LA SEGURIDAD

5.1 Roles: funciones y responsabilidades

Todos los roles y responsabilidades de la organización se encuentran identificados en las fichas de perfil. Estas funciones se han comunicado a todo el personal de la organización.

5.2 Procedimientos de designación

El proceso de asignación se encuentra definido en el procedimiento de gestión de RRHH.

5.3 Procedimientos de resolución de conflictos

El director general y el director de servicios y tecnología son los responsables de la coordinación y de la resolución de conflictos. Cuando se produzca algún conflicto, el afectado lo comunicará por email a su responsable que establecerá las medidas para la resolución de los conflictos y le comunicará el hecho y su resolución a la dirección. En caso de no poder resolver el conflicto, éste será escalado a la propia dirección que tomará las medidas necesarias.

5.4 Política de seguridad de la información

Será misión de Dirección la revisión anual de esta Política de Seguridad y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la dirección y difundida para que la conozcan todas las partes afectadas.

En la declaración de aplicabilidad se establecen las medidas implantadas por la organización para la gestión de todo lo relacionado con la seguridad de la información, así como el nivel establecido. En particular con:

a. Organización e implantación del proceso de seguridad.

a. Análisis y gestión de los riesgos.

b. Gestión de personal.

c. Profesionalidad.

d. Autorización y control de los accesos.

e. Protección de las instalaciones.

f. Adquisición de productos.

g. Seguridad por defecto.

h. Integridad y actualización del sistema.

i. Protección de la información almacenada y en tránsito.

j. Prevención ante otros sistemas de información interconectados.

k. Registro de actividad.

l. Incidentes de seguridad.

m. Continuidad de la actividad.

n. Mejora continua del proceso de seguridad.

6. DATOS DE CARÁCTER PERSONAL

ISBUT trata datos de carácter personal. Todos los sistemas de información de ISBUT 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 registro de actividades de tratamiento de datos.

7. 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

Para la armonización de los análisis de riesgos, la Dirección establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. La Dirección dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8. DESARROLLO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad complementa las políticas de seguridad de ISBUT en diferentes materias:

El listado de las políticas de seguridad se encuentra registrado en el Listado de información documentada.

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 nuestro servidor a disposición de todo el personal.

9. OBLIGACIONES DEL PERSONAL

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

Todos los miembros y colaboradores de ISBUT 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 ISBUT, 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.

10. TERCERAS PARTES

Cuando ISBUT 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 las respectivas directivas y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando ISBUT 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 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.