Binter Sistemas NT

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Sistema Binter

Código: BS-POL-PGS.06.01
Clasificación: PÚBLICA

INDICE

Capitulo Página

1. INTRODUCCIÓN 3

2. ALCANCE 3

3. OBJETIVOS Y FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN 4

4. REQUISITOS MÍNIMOS DE SEGURIDAD 4

5. ROLES, RESPONSABILIDADES Y DEBERES 8

5.1. USUARIOS 9
5.2. ÓRGANOS DE ADMINISTRACIÓN Y DIRECCIÓN 9

6. CONCIENCIACIÓN Y FORMACIÓN 9

7. MARCO LEGAL Y REGULATORIO 10

8. DOCUMENTACIÓN DE SEGURIDAD 10

9. REVISIÓN Y AUDITORÍAS 10

1. INTRODUCCIÓN

Entre las responsabilidades que asumimos, una de las más importantes es la de corresponder a la confianza depositada en nosotros por nuestros clientes y por la sociedad en general. En este contexto, la seguridad de la información que manejamos y gestionamos adquiere una especial relevancia.

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su tratamiento.

Seguridad de la Información es la protección de este activo, asegurando la continuidad del negocio, minimizando los riesgos y contribuyendo a maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos, en el que es fundamental la máxima colaboración e implicación de todos.

Los órganos de administración y de dirección, conscientes del valor de la información, están profundamente comprometidos con la política descrita en este documento.

2. ALCANCE

La presente Política de Seguridad de la Información es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información incluyendo a:

- Miembros de los órganos de administración y dirección.
- Sociedades y organizaciones vinculadas por una relación de control efectivo o cuya gestión y/o administración esté encomendada, con independencia del título en que se funde, a cualesquiera sociedades de la organización.
- A todos los empleados y directivos.
- A todos los usuarios de los sistemas de información.

3. OBJETIVOS Y FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN

- La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción.
- En la protección de la información y los activos relacionados se considera su disponibilidad, integridad y confidencialidad así como la autenticidad de quien accede y la trazabilidad del uso que se realiza.
- Se garantiza la confidencialidad de la información evitando el acceso y la difusión a toda persona no autorizada.
- Se asegura la integridad de la información evitando la manipulación, alteración o borrado accidentales o no autorizados.
- Se salvaguarda la disponibilidad de la información de forma que los usuarios y sistemas que lo requieran puedan acceder a la misma de forma adecuada para el cumplimiento de sus tareas y siempre que ello sea necesario.
- Todos los usuarios tienen la obligación y el deber de custodiar y proteger la información.
- Se garantiza la protección de los datos de carácter personal de acuerdo con el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.
- La información se clasifica de acuerdo a la sensibilidad requerida en su tratamiento y a los niveles de protección exigibles.

4. REQUISITOS MÍNIMOS DE SEGURIDAD

El contenido de esta Política de Seguridad de la Información se desarrolla en normas y procedimientos complementarios atendiendo a los siguientes requisitos mínimos:

a) La seguridad compromete a todos los miembros de la organización.
b) La política y la normativa complementaria de seguridad, identifica unos claros responsables del cumplimiento.
c) La gestión de la seguridad de la información requiere del análisis y tratamiento de los riesgos que afectan a la información y los servicios. El análisis de riesgos se realiza utilizando una metodología reconocida internacionalmente.

d) Las medidas adoptadas para mitigar o suprimir los riesgos están justificadas y, en todo caso, existe una proporcionalidad entre ellas, los riesgos y los costes implicados.
e) Todo el personal debe estar formado e informado de sus deberes y obligaciones en materia de seguridad y sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.
f) El personal relacionado con la información y los sistemas debe aplicar los principios de seguridad en el desempeño de su cometido.
g) Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única.
h) La seguridad de los sistemas debe estar atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida.
i) El personal debe recibir la formación específica necesaria para garantizar la seguridad de la información, los sistemas y los servicios.
j) El acceso a la información debe ser controlado y está limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.
k) Los sistemas se deben instalar en áreas adecuadas y protegidas para garantizar la seguridad de la información tratada. Los sistemas críticos se instalarán en zonas especialmente protegidas y dotadas con control de acceso.
l) Las contrataciones y adquisiciones que supongan acceso a la información deben realizarse amparadas por un contrato que incluya clausulas destinadas a garantizar la salvaguarda de la seguridad de la información y el cumplimiento de la legislación de protección de datos personales.
m) Las organizaciones y las personas que con motivo de contrataciones o adquisiciones de cualquier tipo accedan a la información de la organización, deben conocer la Política de Seguridad de la Información y las normas que sean de aplicación para el objeto de la contratación.
n) En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se debe valorar positivamente, de forma proporcionada a la criticidad del sistema y al nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.
o) Respecto a la seguridad por defecto y por diseño:

a. En el diseño, desarrollo, instalación y explotación de los sistemas de información se deben tener en cuenta y aplicarse los conceptos de seguridad por defecto y desde el diseño.
b. Se debe considerar el estado de la técnica, el coste de la aplicación, la naturaleza, el ámbito de uso, el contexto, los fines u objetivos y los riesgos para determinar los requisitos de seguridad y los controles aplicables.
c. Todos los proyectos que afecten a los sistemas de información deben incluir, en su proceso de análisis, una evaluación de los requisitos de seguridad y de los riesgos y definir un modelo de seguridad consensuado con el Responsable de Seguridad de la Información.
d. Los sistemas deben diseñarse y configurarse de forma que:
    i. El sistema proporcione la mínima funcionalidad requerida para que la organización alcance sus objetivos
    ii. Las funciones de operación, administración y registro de actividad son las mínimas necesarias, y se asegura que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
    iii. En un sistema de explotación se elimina o desactiva, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
    iv. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

p) La estrategia de protección debe estar constituida por múltiples capas de seguridad, dispuestas de forma que, cuando una de las capas falle, permita:
    a. Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
    b. Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
    c. Minimizar el impacto final sobre el mismo.
q) Todo elemento, físico o lógico, requiere autorización previa a su instalación en el sistema. Se debe conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las

vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar los riesgos.

r) Respecto a la información almacenada y en tránsito:
   a. Se debe prestar especial atención a la seguridad de la información almacenada o en tránsito a través de entornos inseguros.
   b. Tienen la consideración de entornos inseguros los equipos portátiles, dispositivos móviles, periféricos, soportes de información y las comunicaciones sobre redes abiertas o con cifrado débil.
   c. Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica deberá estar protegida con el mismo grado de seguridad que ésta.

s) El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas y se deben analizar los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y controlar el punto de unión.

t) Se registran las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas.

u) Respecto a los incidentes de seguridad y su prevención, detección y posterior recuperación:
   a. La seguridad contempla los aspectos de prevención, detección y corrección, para conseguir que las amenazas no se materialicen y no afecten gravemente a la información que se maneja, o los servicios que se prestan.
   b. Se establece un sistema de detección y reacción frente a código dañino.
   c. Se dispone de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se emplea para la mejora continua de la seguridad del sistema.
   d. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplan, entre otros aspectos, la disuasión y la reducción de la exposición.

e. Las medidas de detección deben estar acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen y solucionen a tiempo.
f. Las medidas de recuperación permiten la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.
g. El sistema garantiza la conservación de los datos e informaciones en soporte electrónico.

v) Los usuarios son responsables de informar, de forma inmediata, de cualquier incidente de seguridad, a través de los canales y procedimientos definidos en la organización para la comunicación de incidencias.
w) Se dispone de mecanismos para garantizar la continuidad de la actividad de la organización en caso de contingencia con los sistemas de tratamiento de la información.
x) Para asegurar la mejora continua del proceso de seguridad se implanta un sistema de gestión de seguridad de la información basado en el estándar UNE-ISO/IEC 27001.

5. ROLES, RESPONSABILIDADES Y DEBERES

Los roles, autoridades, responsabilidades y deberes en seguridad de la información se definen, documentan y asignan en “BS-PGS.06.04 Roles y Responsabilidades” que complementa a esta Política de Seguridad de la Información y que también establece el procedimiento para los nombramientos y para la resolución de conflictos.

La Dirección asigna, renueva y comunica las responsabilidades, autoridades y roles en lo referente a la seguridad de la información. También se asegura de que los usuarios conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados, resolviendo los conflictos que se generen en relación a cada responsabilidad.

Al asignar las responsabilidades, autoridades y roles se considera la seguridad como función diferenciada. La responsabilidad de la seguridad de los sistemas de información está diferenciada de la responsabilidad sobre la prestación de los servicios.

La estructura organizativa incluye:

- El gobierno con las funciones de responsable del tratamiento, responsable de la información y responsable del servicio, lo asume la Dirección de la organización.
- La supervisión que corresponde al Responsable de Seguridad de la Información.
- La operación que corresponde al Responsable del Sistema.

5.1. USUARIOS

Los usuarios tienen la obligación de:

1. Conocer y cumplir la Política de Seguridad de la Información y el resto de normas y procedimientos de seguridad aplicables.
2. Mantener la obligación de secreto y proteger y custodiar la confidencialidad, integridad y disponibilidad de la información.
3. Comunicar cualquier incidente de seguridad a través de los canales establecidos para la comunicación de incidencias.

5.2. ÓRGANOS DE ADMINISTRACIÓN Y DIRECCIÓN

Los órganos de administración y de dirección están profundamente comprometidos con la política descrita en este documento y son conscientes del valor de la información y del grave impacto económico y de imagen que puede producir un incidente de seguridad. Asumen la responsabilidad de demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información y de fomentar una cultura corporativa de seguridad de la información.

También se aseguran de que están disponibles los recursos necesarios para el cumplimiento de la política de seguridad de la información y para el funcionamiento del sistema de gestión de seguridad de la información.

6. CONCIENCIACIÓN Y FORMACIÓN

La presente Política de Seguridad de la Información debe ser conocida por todos los usuarios internos y externos y por las entidades que accedan, gestionen o traten datos de la organización.

El conjunto de políticas, normas y procedimientos complementarios a esta Política también deben ser adecuadamente comunicados y puestos en conocimiento de las personas u organizaciones afectadas o implicadas.

Se presta la máxima atención a la concienciación de las personas para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad. Para ello se definen y realizan, periódicamente, acciones de comunicación, concienciación y formación en seguridad de la información.

7. MARCO LEGAL Y REGULATORIO

La creciente importancia de las tecnologías de la información y las comunicaciones en la sociedad han obligado al desarrollo de leyes específicas que garanticen los derechos de los ciudadanos y establezcan requisitos de seguridad en las redes y sistemas, al menos en aquellos sectores críticos para el buen funcionamiento económico y social.

El marco legal y regulatorio de aplicación incluye la legislación aplicable de protección de infraestructuras críticas y servicios esenciales, la protección de los datos personales, la sociedad de la información, el Esquema Nacional de Seguridad o la seguridad de la aviación civil y está detallado en el documento “BS-PGS.06.11 Legislación Aplicable y Requisitos Contractuales” que complementa a esta Política de Seguridad de la Información.

8. DOCUMENTACIÓN DE SEGURIDAD

La documentación asociada a la seguridad de la información y su sistema de gestión se organiza, codifica y gestiona de acuerdo a lo establecido en BS-PAS.01 Control de la Documentación.

9. REVISIÓN Y AUDITORÍAS

Las medidas de seguridad se reevalúan y actualizan periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

El Responsable de Seguridad de la Información revisa esta política anualmente o cuando hay cambios significativos que así lo aconsejen.

Las revisiones tienen en cuenta los cambios en el contexto de la organización, la evolución de la tecnología y la efectividad de la política.

El sistema de gestión de seguridad de la información se audita cada año, según un plan de auditorías establecido y aprobado.