POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Sistema Binter

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

INDICE

1. INTRODUCCIÓN

En el Sistema Binter, entre las responsabilidades que asumimos está 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 tratamos tiene una especial relevancia.

La información es un activo crítico, esencial y de un gran valor que debe ser protegido frente a las amenazas que puedan afectarle.

La seguridad de la información es un proceso que requiere medios técnicos y humanos 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 y 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 protege la confidencialidad de la información evitando el acceso y la difusión a toda persona no autorizada.
- Se protege 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 autorizados puedan acceder a ella siempre que 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 la legislación vigente.
- La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, del sistema.
- La información se clasifica de acuerdo a la sensibilidad requerida en su tratamiento y a los niveles de protección exigibles.
- La seguridad de la información está presente en todos los procesos y actuaciones. Los requisitos de seguridad se aplican en toda la organización.
- Se aplica un ciclo de mejora continua para conseguir los niveles más altos de madurez en el proceso de seguridad de la información, siempre atendiendo a la normativa vigente y a las mejores prácticas.

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, identifican unos claros responsables del cumplimiento.
c) La gestión de los riesgos es parte esencial del proceso de seguridad, por lo que constituye una actividad continua y permanentemente actualizada. El análisis de riesgos se realiza utilizando una metodología reconocida.
d) La gestión de los riesgos permite el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información, de los servicios y de los riesgos a los que estén expuestos.
e) El personal debe estar formado e informado de sus deberes y obligaciones y sus actuaciones supervisadas para verificar que se cumplen los procedimientos.
f) Todos los usuarios están obligados a 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 está 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) Los acuerdos con terceros deben realizarse amparadas por un contrato que incluya clausulas destinadas a garantizar la seguridad de la información y el cumplimiento de la legislación de protección de datos personales.
m) Todos los usuarios que accedan a la información de la organización, deben conocer la Política de Seguridad de la Información y las normas que sean de aplicación según sus roles y funciones asignadas.
n) En la adquisición de productos de seguridad se debe valorar, de forma proporcionada a la criticidad del sistema y al nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad, salvo en los 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 y desarrollo de los sistemas se tienen en cuenta y se aplican los conceptos de seguridad por defecto y desde el diseño.
    b. Se considera 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.
    c. Los proyectos que afecten a los sistemas de información incluyen, en su proceso de análisis, una evaluación de los requisitos de seguridad y de los riesgos y se define un modelo de seguridad consensuado con el Responsable de Seguridad de la Información.
    d. Los sistemas se diseñan y configuran otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica que:
        i. El sistema proporciona la funcionalidad imprescindible.
        ii. Las funciones de operación, administración y registro de actividad son las mínimas necesarias, y sólo pueden realizarse por personas autorizadas, desde emplazamientos o equipos autorizados.
        iii. Se eliminan o desactivan, mediante el control de la configuración, las funciones que son innecesarias o inadecuadas.

iv. El uso del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente.
v. Se aplican guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema.

e. La estrategia de protección incluye múltiples capas de seguridad.

p) La inclusión de cualquier elemento físico o lógico o su modificación requiere autorización formal previa.

q) La evaluación y monitorización son permanentes permitiendo la detección temprana de cualquier incidente y adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten.

r) Se presta especial atención a la seguridad de la información almacenada o en tránsito a través de entornos inseguros. Tienen esta consideración de entornos inseguros los equipos y dispositivos portátiles o móviles, los soportes extraíbles y las comunicaciones sobre redes abiertas o con cifrado débil.

s) Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica se protege con el mismo grado de seguridad que ésta.

t) Se protege el perímetro de los sistemas de información, en particular, si se conectan a redes públicas.

u) Se analizan los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlan los puntos de unión.

v) Se registran las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

w) En la medida estrictamente necesaria y proporcionada, se analizan las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir daños a las redes y sistemas de información.

x) Respecto a los incidentes de seguridad y su prevención, detección y posterior recuperación:

a. Se realizan acciones de prevención, detección y respuesta, al objeto de minimizar las vulnerabilidades y lograr que las amenazas sobre los sistemas no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

b. Las medidas de prevención deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.
c. Las medidas de detección van dirigidas a descubrir la presencia de un ciber incidente.
d. Las medidas de respuesta están orientadas a la restauración de la información y los servicios que pudieran verse afectados por un incidente.
e. El sistema de información garantiza la conservación de los datos e información en soporte electrónico.
f. Se dispone de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
g. Las medidas de detección están acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen y solucionen a tiempo.
h. Las medidas de recuperación permiten la restauración de la información y los servicios tras un incidente de seguridad.

y) Los usuarios son responsables de informar, de forma inmediata, de cualquier incidente de seguridad, a través de los canales y procedimientos establecidos.
z) Se dispone de mecanismos para garantizar la continuidad de la actividad de la organización en caso de contingencia con los sistemas de tratamiento.
aa) Se ha implantado un sistema de gestión de seguridad de la información basado en ISO/IEC 27001 para asegurar la mejora continua del proceso de seguridad.

5. ROLES, RESPONSABILIDADES Y DEBERES

Los roles, autoridades, responsabilidades y deberes en seguridad de la información se definen, documentan y asignan en el documento "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 obligación, entre otras cosas, de conocer y cumplir la Política de Seguridad de la Información y el resto de normas y procedimientos de seguridad aplicables, mantener la obligación de secreto y proteger y custodiar la confidencialidad, integridad y disponibilidad de la información y 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 son conscientes del valor de la información y del grave impacto 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 de los sistemas de información. El conjunto de políticas, normas y procedimientos complementarios a esta Política también deben ser 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

El Sistema Binter se compromete a a cumplir la legislación aplicable, considerar las normas pertinentes y las mejores prácticas.

El marco legal y regulatorio 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 los procedimientos aprobados de control de la documentación.

9. REVISIÓN Y AUDITORÍAS

Las medidas de seguridad se reevalúan y actualizan periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

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.