Bjumper

Ilustración 1

Política de Seguridad

Índice de contenidos

1. Aprobación y entrada en vigor 4
2. Misión de la organización 4
3. Alcance 5
4. Objetivos 5
5. Marco normativo 5
6. Desarrollo 6
7. Organización de la seguridad 7
8. Estructuración, gestión y acceso a la documentación de seguridad. 7
9. Comité de seguridad 8
10. Resolución de Conflictos 9
11. Gestión de riesgos 9
12. Gestión de personal 9
13. Profesionalidad y seguridad de los recursos humanos 10
14. Autorización y control de acceso a los sistemas de información 11
15. Protección de las instalaciones 12
16. Adquisición de componentes de seguridad 13
17. Seguridad por defecto 13
18. Integridad y actualización del sistema 13
19. Protección información almacenada y en tránsito 14
20. Prevención de sistemas de información interconectados 14
21. Registros de actividad 15
22. Gestión de incidentes 15
23. Continuidad de la actividad 15
24. Mejora continuidad del proceso de seguridad 16

Copyright © 2025 Bjumper. Todos los derechos Reservados.

Control de Cambios

Edición	Fecha	Modificaciones
1.0	**30/01/2025**	**Edición inicial**

Copyright © 2025 Bjumper. Todos los derechos Reservados.

1. Aprobación y entrada en vigor

La Política de Seguridad de la Información es efectiva desde la fecha de firma y hasta que sea reemplazada por una nueva Política.

2. Misión de la organización

BJUMPER es consciente de la importancia de los sistemas TIC (tecnologías de Información y comunicaciones) para alcanzar sus objetivos y asume su compromiso con la seguridad de la información, somete a la adecuada de los mismos, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

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 que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar 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.

Copyright © 2025 Bjumper. Todos los derechos Reservados.

Los departamentos deben estar preparados para prevenir, vigilar, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS (Artículo 8. Prevención, detección, respuesta y conservación. Real Decreto 311/2022, de 3 de mayo de 2022, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica)

3. Alcance

Esta política se aplica a todos los sistemas TIC de la entidad y a todos los miembros de la organización, implicados en la prestación de servicios audiovisuales de ingeniería y soporte a clientes externos que requieran la aplicación de ENS, sin excepciones.

4. Objetivos

Por todo lo anteriormente expuesto, la Dirección establece los siguientes objetivos de seguridad de la información:

- Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.
- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico y/o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.
- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

5. Marco normativo

Uno de los objetivos debe ser el de cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribimos además de los compromisos adquiridos

Copyright © 2025 Bjumper. Todos los derechos Reservados.

con los clientes, así como la actualización continua de los mismos. Para ello, el marco legal y regulatorio en el que desarrollamos nuestras actividades es:

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Real Decreto 311/2022, de 3 de mayo, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

6. Desarrollo

Para poder lograr estos objetivos es necesario:

- Mejorar continuamente nuestro sistema de seguridad de la información.
- Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, puedan causar.
- Preservar los intereses de sus principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.
- Trabajar de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.
- Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.

Copyright © 2025 Bjumper. Todos los derechos Reservados.

- Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.

7. Organización de la seguridad

La responsabilidad esencial recae sobre la Dirección de la organización, ya que ésta es responsable de organizar las funciones, responsabilidades y de facilitar los recursos adecuados para conseguir los objetivos del ENS. Los directivos son también responsables de dar buen ejemplo siguiendo las normas de seguridad establecidas.

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándose y poniéndolos en público conocimiento a través de la presente Política Integrada de Sistemas de Gestión.

8. Estructuración, gestión y acceso a la documentación de seguridad.

Los documentos que integran el Sistema de Gestión se encuentran a disposición del personal (siguiendo el principio de “necesidad de conocer”) en soporte digital, para su consulta, sin posibilidad de modificación. Dicha documentación será accesible por el personal en la plataforma de comunicación interna y/o directorio SGSI de la red privada de BJUMPER.

La documentación de seguridad se estructura en:

- Política de Seguridad.
- Normativa de seguridad: documentos que describen el uso de equipos, servicios e instalaciones.

Copyright © 2025 Bjumper. Todos los derechos Reservados.

- Describen lo que se considera uso indebido, la responsabilidad del personal con respecto al cumplimiento o violación de la normativa, derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.
- Documentos específicos: documentación de seguridad desarrollada según las guías CCN-STIC que resulten de aplicación.
- Procedimientos de seguridad: documentos que detallan cómo operar los elementos del sistema.

La gestión de la documentación de seguridad conlleva su mantenimiento, actualización, revisión y aprobación, y será llevada a cabo por el Responsable del Sistema y el Comité de Seguridad.

9. Comité de seguridad

El procedimiento para su designación y renovación será la ratificación en el comité de seguridad.

El comité para la gestión y coordinación de la seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité.

Los miembros del comité de seguridad de la información son:

- Responsable de la Información
- Responsable de los Servicios
- Responsable de la Seguridad
- Responsable de Sistemas.

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos.

El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de nuestra empresa.

Copyright © 2025 Bjumper. Todos los derechos Reservados.

10. Resolución de Conflictos

En caso de conflicto entre los roles establecidos en la presente Política de Seguridad respecto al cumplimiento y desarrollo de las funciones y tareas que tienen asignadas, éste será resuelto por su superior jerárquico común teniendo en consideración aquella decisión que presente un mayor nivel de exigencia respecto a la protección de datos de carácter personal. Si no existiera, deberá resolver el Comité de Seguridad.

11. 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 revisa 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.

Para la realización del análisis de riesgos se tendrá en cuenta la metodología de análisis de riesgos desarrollada en el procedimiento Análisis de Riesgos.

12. Gestión de personal

Todo el personal de BJUMPER bajo el alcance del ENS tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo

Copyright © 2025 Bjumper. Todos los derechos Reservados.

responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

El personal de BJUMPER realizará acciones de concienciación en materia de seguridad TIC regularmente. Se establecerá un programa de concienciación continua para atender a todo el personal de la organización, 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.

13. Profesionalidad y seguridad de los recursos humanos

Esta Política se aplica a todo el personal de la organización y el personal externo que realiza tareas dentro de la empresa.

El área de RRHH incluirá funciones de seguridad de la información en las descripciones de los trabajos de los empleados, informará a todo el personal que contrate sus obligaciones con respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los compromisos de confidencialidad con el personal y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

El Responsable de Seguridad (RGS) [CISO], es responsable de monitorear, documentar y analizar los incidentes de seguridad reportados, así como de comunicarse al Comité de Seguridad de la Información y a los propietarios de información.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad (RGS) [CISO] maneje informes de incidentes y anomalías del sistema. El Comité también estará al tanto, supervisará la investigación, supervisará la evolución de la información y promoverá la resolución de incidentes de seguridad de la información.

Todo el personal de la organización es responsable de informar sobre las debilidades e incidentes de seguridad de la información que se detectan oportunamente.

Copyright © 2025 Bjumper. Todos los derechos Reservados.

Profesionalidad de los recursos humanos:

- Determinar la competencia necesaria del personal para llevar a cabo el trabajo que afecta a la Seguridad de la Información
- Hay que asegurar que las personas sean competentes sobre la base de la educación, capacitación o experiencia adecuadas
- Demostrar mediante la información documentada que sea necesaria la competencia del personal en materia de Seguridad de la Información

Los objetivos de controlar la seguridad del personal son:

- Reducir los riesgos de error humano, puesta en marcha de irregularidades, uso indebido de instalaciones y recursos, y manejo no autorizado de la información.
- Explicar las responsabilidades de seguridad en la etapa de reclutamiento del personal e incluirlas en los acuerdos a firmar y verificar su cumplimiento durante el desempeño de las tareas del empleado.
- Asegúrese de que los usuarios estén al tanto de las amenazas y preocupaciones de seguridad de la información y estén capacitados para apoyar la Política de Seguridad de la Información de la organización en el curso de sus tareas normales.
- Establecer compromisos de confidencialidad con todo el personal y usuarios fuera de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de las debilidades de seguridad existentes, así como los incidentes, con el fin de minimizar sus efectos y prevenir su reincidencia.

14. Autorización y control de acceso a los sistemas de información

El control del acceso a los sistemas de información tiene por objetivo:

- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de la organización y otras redes públicas o privadas.

Copyright © 2025 Bjumper. Todos los derechos Reservados.

- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.
- Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y ordenadores personales para el trabajo remoto.

15. Protección de las instalaciones

Los objetivos de esta política en materia de protección de las instalaciones son:

- Prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de BJUMPER.
- Proteger el equipo de procesamiento de información crítico de la organización, colocándolo en áreas protegidas y protegido por un perímetro de seguridad definido, con las medidas de seguridad y controles de acceso adecuados. Asimismo, contemplar la protección de esta en su traslado y permanecer fuera de las áreas protegidas, por mantenimiento u otros motivos.
- Controlar los factores ambientales que podrían perjudicar el buen funcionamiento del equipo de cómputo que alberga la información de la organización.
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus tareas habituales.
- Proporcionar protección proporcional a los riesgos identificados.
- Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información de la organización: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.
- El Responsable de Seguridad (RGS), junto con los Responsables de la Información, según proceda, definirá las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos, y supervisará su aplicación. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.
- Los responsables de los diferentes departamentos definirán los niveles de acceso físico del personal de la organización a las áreas restringidas bajo su responsabilidad. Los Propietarios de Información autorizarán formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de la organización cuando lo consideren apropiado.
- Todo el personal de la organización es responsable del cumplimiento de la política de pantalla limpia y escritorio, para la protección de la información relacionada con el trabajo diario en las oficinas.

Copyright © 2025 Bjumper. Todos los derechos Reservados.

16. Adquisición de componentes de seguridad

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 deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por otro lado, se tendrá en cuenta la seguridad de la información en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.

La política de adquisición de componentes de seguridad se desarrolla en el documento “adquisición de componentes de seguridad”.

17. Seguridad por defecto

La organización considera estratégico para la entidad que los procesos integren la seguridad de la información como parte de su ciclo de vida. Los sistemas de información y los servicios deben incluir la seguridad por defecto desde su creación hasta su retirada, incluyéndose la seguridad en las decisiones de desarrollo y/o adquisición y en todas las actividades en explotación estableciéndose la seguridad como un proceso integral y transversal.

18. Integridad y actualización del sistema

BJUMPER se compromete a garantizar la integridad del sistema mediante un proceso de gestión de cambios que permita el control de la actualización de los elementos físicos o lógicos mediante la autorización previa a su instalación en el sistema. Dicha evaluación será llevada a cabo principalmente por la dirección de sistemas que evaluará el impacto en la seguridad del sistema antes de realizar los cambios y controlará de forma

Copyright © 2025 Bjumper. Todos los derechos Reservados.

documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas.

Mediante revisiones periódicas de seguridad se evaluará el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

19. Protección información almacenada y en tránsito

La organización establece medidas de protección para la Seguridad de la Información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

20. Prevención de sistemas de información interconectados

BJUMPER establece medidas de protección para la Seguridad de la Información especialmente para proteger el perímetro, en particular, si se conecta a redes públicas, especialmente si se utilizan en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público.

En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión. Conexiones electrónicas disponibles para el público.

Copyright © 2025 Bjumper. Todos los derechos Reservados.

21. Registros de actividad

La organización registrará 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.

22. Gestión de incidentes

Los objetivos principales de la Gestión de incidentes son:

- Establecer un sistema de detección y reacción frente a código dañino
- Disponer de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
- Estos procedimientos cubrirán 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.
- Garantizar que los servicios de IT vuelvan a tener un desempeño óptimo.
- Reducir los posibles riesgos e impactos que pueda causar el incidente.
- Velar por la integridad de los sistemas en el caso de un incidente de seguridad
- Comunicar el impacto de un incidente tan pronto como se detecte para activar la alarma; y poner en práctica un plan de comunicación empresarial adecuado.
- Promover la eficiencia empresarial.

23. Continuidad de la actividad

La organización con el objetivo de garantizar la continuidad de las actividades establece medidas para que los sistemas dispongan de copias de seguridad y establezcan mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Copyright © 2025 Bjumper. Todos los derechos Reservados.

24. Mejora continuidad del proceso de seguridad

La organización establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en la norma.

52094302S LUIS ALCAZAR (R: B86677416)

Firmado digitalmente por 52094302S LUIS ALCAZAR (R: B86677416)
Fecha: 2025.10.15 18:47:32 +02'00'

Firmado:

Copyright © 2025 Bjumper. Todos los derechos Reservados.