BROAD SERVICE

Política de Seguridad de la Información

Política de Seguridad de la Información

Tabla de Contenido

Contenido

1. Aprobación y entrada en vigor 3
2. Misión de la organización 3
3. Alcance 4
4. Objetivos 4
5. Marco normativo 4
6. Desarrollo 5
7. Organización de seguridad 6
8. Comité de Seguridad 6
9. Gestión de Riesgos 7
10. Gestión de Personal 7
11. Profesionalidad y seguridad de los recursos humanos 7
12. Autorización y control de acceso a los Sistemas de Información 8
13. Resolución de Conflictos 8
14. Protección de datos personales 8
15. Protección de las instalaciones 9
16. Adquisición de productos 9
17. Seguridad por defecto 9
18. Integridad y actualización del sistema 9
19. Protección de la información almacenada y en tránsito 10
20. Prevención de sistemas de información interconectados 10
21. Registros de actividad 10
22. Continuidad de la actividad 11
23. Mejora continua del proceso de seguridad 11
24. Política de Cookies 11

1. Aprobación y entrada en vigor

Esta 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

BROAD SERVICE siendo una empresa dedicada proporcionar a nuestro clientes las mejores soluciones tecnológicas en ingeniería y servicios audiovisuales. Con una amplia trayectoria en el sector de la Televisión/Broadcast, es consciente de la importancia de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos y asumiendo su compromiso con la seguridad de la información, se somete a la adecuación 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..

BROAD SERVICE TECHNICAL SUPPORT para alcanzar sus objetivos asume su compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de esta, 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. 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 proyectos de TIC.
Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS (Artículo 8. Prevención, detección, respuesta y conservación).

3. Alcance

Esta política se aplica a todos los sistemas TIC de la entidad y a todos los miembros de la organización, implicados en Servicios y Proyectos destinados al sector público, que requieran la aplicación de ENS, sin excepciones.

Está política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión de la información.

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 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 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:

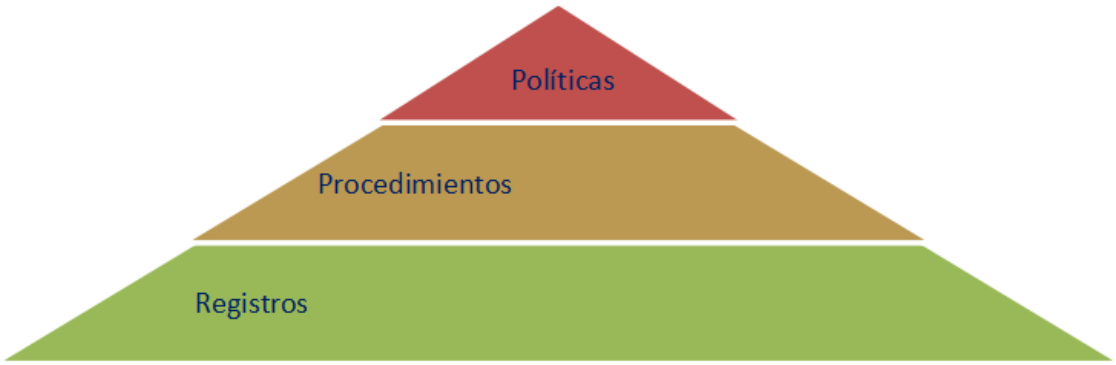
- ➔ REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- ➔ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales 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, por el que se regula el Esquema Nacional de Seguridad.
- ➔ Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- ➔ Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- ➔ Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

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.
- ➔ 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.
- ➔ Estructurar nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión tiene la siguiente estructura:



7. Organización de seguridad

La responsabilidad esencial recae sobre la Dirección General de la organización, ya que esta es responsable de organizar las funciones y 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.

Los roles o funciones de seguridad definidos son:

Función	Deberes y responsabilidades
Responsable de la información (RINFO)	· Tomar las decisiones relativas a la información tratada
Responsable de los servicios (RSER)	· Coordinar la implantación del sistema · Mejorar el sistema de forma continua
Responsable de la seguridad (RSEG o CISO)	· Determinar la idoneidad de las medidas técnicas · Proporcionar la mejor tecnología para el servicio
Responsable del sistema (RSIS)	· Coordinar la implantación del sistema · Mejorar el sistema de forma continua
Dirección	· Proporcionar los recursos necesarios para el sistema · Liderar el sistema
Administrador de Seguridad (AS)	· Implantación, gestión y mantenimiento de las medidas de seguridad.

8. 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 SEGURIDAD
- RESPONSABLE DEL SISTEMA
- RESPONSABLE DEL SERVICIO
- RESPONSABLE DE INFORMACIÓN

9. 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.

10. Gestión de Personal

Todos los miembros de BROAD SERVICE TECHNICAL SUPPORT, tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad.
Todos los miembros de BROAD SERVICE TECHNICAL SUPPORT, atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año.
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.

11. Profesionalidad y seguridad de los recursos humanos

Esta Política se aplica a todo el personal de BROAD SERVICE TECHNICAL SUPPORT, y el personal externo que realiza tareas dentro de la empresa.
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.

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.

12. 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 BROAD SERVICE TECHNICAL SUPPORT y otras redes públicas o privadas.
- 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.

13. 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 de la Información.

14. Protección de datos personales

En lo referente a los datos personales, que sean objeto de tratamiento por los sistemas de información y comunicación de BROAD SERVICE TECHNICAL SUPPORT, se cumplirá con los principios y obligaciones de la normativa vigente en materia de protección de datos, entre otras, el Reglamento (UE) 679/2016, General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución Española. Asimismo, se adoptarán las medidas técnicas y organizativas que corresponda implantar, derivadas de los riesgos generados por el tratamiento, una vez llevado a cabo el análisis de riesgos exigido por el RGPD, y sin perjuicio de aquellas situaciones en las que se requiera con carácter previo realizar una Evaluación de Impacto de la Protección de Datos (EIPD).

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 BROAD SERVICE TECHNICAL SUPPORT
- Proteger el equipo de procesamiento de información crítico de BROAD SERVICE TECHNICAL SUPPORT, 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 BROAD SERVICE TECHNICAL SUPPORT
- 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 BROAD SERVICE TECHNICAL SUPPORT: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

16. Adquisición de productos

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 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.

17. Seguridad por defecto

BROAD SERVICE TECHNICAL SUPPORT 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

BROAD SERVICE TECHNICAL SUPPORT 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 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 de la información almacenada y en tránsito

BROAD SERVICE TECHNICAL SUPPORT 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

BROAD SERVICE TECHNICAL SUPPORT, 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.

21. Registros de actividad

BROAD SERVICE TECHNICAL SUPPORT, 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.

Los objetivos principales de la Gestión de incidentes son los de:

- 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.

22. Continuidad de la actividad

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

23. Mejora continua del proceso de seguridad

BROAD SERVICE TECHNICAL SUPPORT establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en normas internacionales como ISO 27001.

24. Política de Cookies

DATOS IDENTIFICATIVOS
Empresa: BROAD SERVICE TECHNICAL SUPPORT SL
NIF: B82302357
Dirección: C. Margarita Salas, 24, 28919 Leganés, Madrid, España.
Correo electrónico: broadservice@broadservice.es
Sitio web: https://broadservice.es/

De conformidad con lo establecido en la Ley 34/2002 de Servicios de la Sociedad de la Información, te informamos que los sitios web broadservice.es, utiliza cookies. Las cookies son pequeños ficheros de información del sitio web que el Usuario que lo visita almacena en su ordenador o dispositivo.
En general el uso de cookies se regirá según lo establecido en nuestra Política de cookies publicada en nuestras webs:
https://broadservice.es/politica-de-cookies/

En Leganés a 1 de noviembre de 2024

La Dirección General