POLÍTICA DE SEGURIDAD DEL SGSI GUARDEDBOX – ORG.1

POLÍTICAS DE ADECUACIÓN AL ENS:2022/ISO27001

Código:	SOA.ORG.1
Versión:	2.0
Fecha de la versión:	29/10/2024
Creado por:	Responsable de Seguridad
Aprobado por:	Raúl Siles Peláez (CEO)
Nivel de confidencialidad:	CONFIDENCIAL
Número de páginas:	12

HISTÓRICO DE MODIFICACIONES

FECHA	VERSIÓN	AUTOR	DESCRIPCIÓN DE LA MODIFICACIÓN
04/08/22	0.1	Mónica Salas	Primera versión
27/10/24	2.0	Mónica Salas	Actualización

Contents

HISTÓRICO DE MODIFICACIONES 1
1. Objeto 2
2. Alcance 2
3. Objetivos 2
4. Desarrollo 3
5. Responsabilidades 4
6. Organización de la seguridad 4
   6.1. Comité de Seguridad 4
   6.2. Responsable de la Información 5
   6.3. Responsable del Servicio 5
   6.4. Responsable de Seguridad 6
   6.5. Responsable de Sistemas 7
   6.6. Responsable de Desarrollo 7
   6.7. Obligaciones del resto del personal 7
   6.8. Terceras partes 8
7. Gestión de Riesgos 8
8. Política de autorización y control de acceso al SGSI 8
   8.1. Seguridad por defecto 9
   8.2. Gestión de cambios 9
9. Datos de carácter personal 9
10. Requisitos 9
11. Marco normativo 10
12. Estructuración, acceso y control de la documentación de seguridad del SGSI 10
13. Registros de actividad 11
14. Referencias 11
15. Firma del documento 11

1. Objeto

El presente documento forma parte del Sistema de Gestión de Seguridad de la Información (en adelante, SGSI) para la solución GuardedBox.

GuardedBox S.L. ("GUARDEDBOX"), consciente de que la seguridad de la información relativa a nuestros clientes es un recurso fundamental, ha establecido un Sistema de Gestión de la Seguridad de la Información y de Gestión de la Privacidad de acuerdo a los requisitos definidos en la norma ISO/IEC 27001:2022 e ISO 27701:2024 y al Esquema Nacional de Seguridad regulado por el Real Decreto 3/2010, de 8 de enero, en el ámbito de la Administración Electrónica, y modificado por el Real Decreto 311/2022 de 3 de mayo, para garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño, asegurar el cumplimiento de los objetivos fijados y gestionar la Privacidad de los datos personales que el SGSI gestiona.

El objetivo de esta Política de Seguridad de la Información es establecer el marco de actuación necesario, así como sus principios, para proteger los recursos de información frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar los principios de Autenticidad, Trazabilidad, Confidencialidad, Integridad y Disponibilidad de la información.

La Dirección procederá a la revisión periódica de la presente política y su modificación si fuera necesario. Es responsabilidad de toda la organización de GUARDEDBOX el obligado cumplimiento de lo establecido en sus sistemas de calidad y seguridad de la información, y, fundamentalmente, de las personas al cargo de las actividades comprendidas dentro de los citados sistemas, asumiendo las responsabilidades en materia de seguridad y sobre los activos de información a su cargo.

2. Alcance

La Política de Seguridad se aplica a toda la empresa y a sus activos de información, incluyendo:

- Todos los departamentos, tanto directivos como empleados.
- Todos los contratistas que tuvieran acceso a la información o los sistemas de la organización.
- Bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.
- La información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas.
- La información cedida dentro de un marco legal establecido, que será considerada como propia a efectos exclusivos de su protección.
- Todos los sistemas utilizados para administrar y gestionar la información, sean propios o alquilados.

3. Objetivos

La presente Política de Seguridad atiende a los siguientes objetivos de la Organización:

- Asegurar que los servicios prestados y productos suministrados son seguros, fiables, cumplen con los pliegos de condiciones, normas e instrucciones aplicables, se adaptan a los requisitos y expectativas de sus clientes y mejoran continuamente.

- Asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información gestionada.
- Asegurar que los servicios están protegidos contra pérdidas de confidencialidad, integridad, disponibilidad, autenticidad, y trazabilidad.
- Asegurar la capacidad de respuesta ante situaciones de emergencia, restableciendo el funcionamiento de los servicios críticos en el menor tiempo posible.
- Mantener al día la legislación aplicable y cumplir todos los requisitos legales y normativos establecidos en materia de calidad, gestión ambiental y seguridad de la información, asociados a las actividades y aspectos que sean de obligado cumplimiento y también aquellos que Dino Security suscribe voluntariamente.
- Conseguir y mantener el nivel de seguridad requerido para garantizar de forma adecuada la continuidad del negocio, incluso en situaciones adversas.
- Incrementar la integración y el apoyo mutuo de los aspectos físicos y lógicos de la seguridad.
- Establecer la estructura corporativa de seguridad definida por los órganos de decisión de la organización y crear los canales de comunicación adecuados entre todos los implicados.
- Proteger a las personas que trabajan en la empresa, la confidencialidad y disponibilidad de sus comunicaciones y la integridad de su información.
- Velar por los activos que componen el patrimonio de la compañía, en particular, los equipos informáticos o los contenidos de todo género.
- Implicar, motivar y comprometer al personal propio y aquel que trabaje en nombre de Dino Security y GuardedBox S.L., con objeto de buscar su participación en la gestión, desarrollo y aplicación del Sistema de Gestión de la Seguridad de la Información implantado.
- Establecer e implantar planes de formación y divulgación en seguridad para la mejora continua de la formación del personal en materia de Seguridad de la Información.
- Garantizar un proceso de mejora continua en los elementos vinculados a la seguridad de la información y los sistemas, tratando las métricas recogidas y detectando elementos sobre los que se debe actuar.
- Detectar desviaciones sobre los objetivos, analizar las causas, y tomar las acciones pertinentes para corregirlas.

4. Desarrollo

Para lograr estos objetivos, es necesario:

- Mejorar continuamente nuestro SGSI.
- Identificar las amenazas potenciales, y el potencial impacto en las operaciones de negocio que, caso de materializarse, puedan causar.
- Preservar los intereses de las principales partes interesadas (clientes, usuarios, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.
- Colaborar con nuestra cadena de suministro 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 periódicamente y garantizar la competencia técnica del personal, así como asegurar su implicación en la mejora continua de nuestros procesos, proporcionando

las adecuadsa formación y comunicación interna para que desarrollen buenas prácticas definidas en el sistema.
- Garantizar el correcto estado de las instalaciones y demás recursos asociados al servicio, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- Analizar de manera continua de todos los procesos relevantes, identificando áreas de mejora, en función de los resultados obtenidos y de los objetivos establecidos.
- Estructurar el SGSI de forma que sea fácil de comprender.

5. Responsabilidades

La responsabilidad de la seguridad de la información involucrada en la prestación de los servicios incluidos en el alcance del SGSI es de la Dirección, que pondrá los medios adecuados, sin perjuicio de que los empleados o usuarios asuman su parte de responsabilidad respecto a los medios que utiliza, según lo indicado en las normativas y en los procedimientos complementarios.

En el apartado "6. Organización de la seguridad" se describe los roles y sus responsabilidades en la organización de la seguridad de GUARDEDBOX.

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad.

La Dirección analizará los riesgos y vulnerabilidades en materia de seguridad que puedan afectar al buen funcionamiento del negocio y propondrá las normas, medios y medidas procedentes para suprimirlos y, en su defecto, minimizarlos. A estos efectos, también estudiará los posibles riesgos ambientales.

El personal de GUARDEDBOX deberá conocer las normas, reglas, estándares y procedimientos relacionados con su puesto de trabajo, así como sus funciones y obligaciones, además de la separación de funciones y la revisión independiente de los registros, cuando sea necesario, de quién ha hecho qué, cuándo y desde dónde.

Todos los empleados de GUARDEDBOX están obligados a comunicar las incidencias de seguridad. Los responsables se asegurarán de que dichas incidencias sean tratadas apropiadamente.

6. Organización de la seguridad

6.1. Comité de Seguridad

Es responsabilidad del comité de seguridad la coordinación de la seguridad de la información en GUARDEDBOX. Estará formado por:

- La Dirección de la Empresa (socios).
- El Responsable de la Información.
- El Responsable del Servicio.
- El Responsable de Seguridad.
- El Responsable de Sistemas.
- El Responsable de Desarrollo.

Todos los cargos anteriores se nombran por parte de la Dirección.

El Comité de Seguridad reportará al Director General. Se reunirá semestralmente (y cada vez que se requiera por parte de la Dirección o por parte del Responsable de Seguridad).

Es su responsabilidad revisar regularmente la Política de Seguridad de la información y someterla a aprobación por parte de la organización.

6.2. Responsable de la Información

Será el propietario de la misma, y tendrá las siguientes funciones:

- Clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (confidencialidad, integridad, disponibilidad, autenticidad, y trazabilidad), dentro del marco establecido en el Anexo I del ENS.
- Trabajar en colaboración con el Responsable de Seguridad y el del Sistema en el mantenimiento de los servicios de administración electrónica catalogados.
- Apoyar la realización de los análisis de riesgos y valorar las diferentes opciones de gestión del riesgo a implantar.
- Llevar a cabo el análisis de riesgos, conjuntamente con el Responsable de Seguridad.
- Evaluar potenciales nuevos criterios de clasificación de la información según su nivel de criticidad, conjuntamente con el Responsable de Seguridad.
- Protección de la información almacenada y en tránsito.
- Valorar y decidir, junto con los Responsables del Servicio, los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes que puedan tener acceso a información de los procedimientos administrativos que gestiona y realizar el seguimiento de su cumplimiento
- Establecer el mecanismo de registro de actividad para asegurar el cumplimiento de las medidas de seguridad con las garantías de los derechos a la intimidad personal.

6.3. Responsable del Servicio

Será quien determine los requisitos de los servicios prestados, y tendrá las siguientes funciones:

- Determinar los niveles de seguridad de los servicios, estableciendo sus requisitos en materia de seguridad.
- Clasificar los servicios conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (confidencialidad, integridad, disponibilidad, autenticidad, y trazabilidad), dentro del marco establecido en el Anexo I del ENS.
- Atender a los requisitos de seguridad de la información, tales como confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, etc., que se demanden en la prestación de los servicios.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes que puedan afectar a sus servicios y realizar el seguimiento de su cumplimiento.

- Adquirir los productos necesarios para la correcta prestación de cada servicio, respetando los requisitos de seguridad establecidos en la presente política.
- Asegurar la continuidad de la actividad ante cualquier eventualidad.
- Definir los mecanismos de autorización y control de los accesos.
- Llevar a cabo la gestión de personal, incluyendo la toma de decisiones relativas a la contratación de las personas adecuadas para cada perfil.
- Definir las medidas de protección de las personas en el desempeño de sus funciones.
- Verificar la aplicación de los Procedimientos Operativos de Seguridad (POS).

6.4. Responsable de Seguridad

Será quien tome las decisiones adecuadas para satisfacer los requisitos de seguridad de la información y de los servicios, y tendrá las siguientes funciones:

- Supervisar el cumplimiento de la presente Política de Seguridad, de sus normas y procedimientos derivados.
- Asesorar en materia de seguridad a los integrantes Comité de Seguridad que así lo requieran.
- Organizar e implantar el proceso de seguridad por defecto.
- Disponer del conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
- Elaborar los Procedimientos Operativos de Seguridad (POS) en colaboración con el Responsable de Desarrollo.
- Asesorar, en colaboración con los responsables de Sistemas, del Servicio y de la Información, en la realización del análisis y gestión de riesgos, elevando el informe resultante al Comité de Seguridad.
- Definir los protocolos necesarios para monitorizar el estado de seguridad del sistema.
- Monitorizar los resultados proporcionados por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones Comité de Seguridad en materia de seguridad.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.
- Elaboración y revisión de la normativa de seguridad Comité de Seguridad.
- Aprobación de los procedimientos de seguridad elaborados por el Responsable de Sistemas.
- Asegurar los recursos necesarios para la implementación y mantenimiento del SGSI.
- Analizar los incidentes de seguridad y notificar inmediatamente a las autoridades competentes.
- Realizar el seguimiento de la implementación y seguimiento de los controles.
- Establecer mecanismos para la mejora continua del proceso de seguridad.
- Definir las políticas de formación del personal en materia de seguridad y velar por su cumplimiento.

La responsabilidad general de la seguridad de la información recaerá sobre el Responsable de Seguridad, siendo la responsabilidad última del Comité de Seguridad y de la Dirección como

máximo responsable del SGSI. El detalle de la composición del Comité de Seguridad, así como las obligaciones de cada rol en el ámbito de la seguridad de la información se determina actas del propio comité.

6.5. Responsable de Sistemas

Cada responsable de un sistema de información tendrá asignadas, dentro de sus áreas de actuación, las siguientes funciones:

- Implantación, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del SGSI.
- Elaborar procedimientos operativos de seguridad de los sistemas de información.
- Elaborar planes de continuidad de los sistemas de información.
- Colaborar para la realización del análisis de riesgos de los sistemas de información de los que es responsable.
- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información.
- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información, en colaboración con los Responsables del Servicio y de Desarrollo.
- Prevención de los riesgos derivados de la interconexión con otros sistemas de información.
- Definir las medidas de protección de las instalaciones.

6.6. Responsable de Desarrollo

- Elaborar los Procedimientos Operativos de Seguridad (POS) en colaboración con el Responsable de Seguridad.
- Evaluar y gestionar un ciclo de vida de desarrollo del software seguro para todos los componentes software de las soluciones propias del entorno.
- Gestionar la seguridad de los componentes de terceros involucrados en los desarrollos propios.
- Velar por el cumplimiento de los procedimientos establecidos para asegurar la calidad del software, el correcto modelo de puesta en producción, y los procedimientos para detectar y corregir fallos en él.
- Dirigir la actividad del equipo de Desarrollo, concienciando y velando por la buenas prácticas, y establecer modelos de control que detecten y corrijan desviaciones.

6.7. Obligaciones del resto del personal

- Todos los miembros de Dino Security y GuardedBox tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados en el momento de su incorporación y siempre que tenga lugar una actualización relevante.

- 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 es obligatoria antes de asumir una responsabilidad, tanto para la primera asignación como ante cambio de puesto de trabajo o de responsabilidades en el mismo.

6.8. Terceras partes

- Dino Security / GuardedBox pondrán en conocimiento de cualquier organismo que contrate el servicio esta Política de Seguridad de la Información, bajo petición expresa.
- Dino Security / GuardedBox establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción y respuesta ante incidentes de seguridad.
- Cuando Dino Security / GuardedBox utilicen servicios de terceros, evaluarán su conformidad con el ENS y/o su SGSI (ej. ISO/IEC 27001), y, en caso de no estar certificados o ser conformes, les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios, en función de los acuerdos de colaboración.
- 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.

7. Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán someterse a un análisis de riesgos, que contemple las amenazas y los riesgos a los que están expuestos. Este análisis se revisa atendiendo a las siguientes condiciones:

- al menos una vez al año;
- ante cambios en la información manejada;
- ante modificaciones relevantes en los servicios;
- al desplegar nuevas versiones que impliquen cambios criptográficos;
- si acontece un incidente grave de seguridad;
- si alguna auditoría de seguridad identifica vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC 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.

8. Política de autorización y control de acceso al SGSI

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 GUARDEDBOX y otras redes públicas o privadas.
- Auditar y 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.

8.1. Seguridad por defecto

GUARDEDBOX 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.

8.2. Gestión de cambios

GUARDEDBOX se compromete a garantizar la integridad del sistema mediante un proceso formal de gestión de cambios que permita el control de la actualización de los elementos físicos o lógicos mediante la autorización previa a su introducción en el entorno. Dicha evaluación será llevada a cabo directamente por la dirección técnica, previa realización de una evaluación de impacto en la seguridad del sistema, documentando de manera formal todos los cambios que se clasifiquen como importantes o con implicaciones en la seguridad del SGSU.

El estado de seguridad de los sistemas se someterá a revisiones periódicas de seguridad según las especificaciones de los fabricantes, las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo.

9. Datos de carácter personal

- La política de privacidad se encuentra descrita en https://guardedbox.es/terms.html#privacy.
- Los usuarios de la solución GuardedBox pueden consultar cualquier duda que les surja en relación con tratamiento de sus datos, así como ejercer todos sus derechos legales en relación a los mismos, contactando con el responsable de protección de datos en la dirección dpo(@)guardedbox.es.
- Todos los datos personales se almacenan en la plataforma www.guardedbox.com, certificada en cumplimiento con el ENS en categoría ALTA. El producto que la sustenta, GuardedBox, es un producto cualificado en el catálogo CPSTIC-CCN-STIC 105 para compartición online - Familia "Cifrado y compartición segura de información".

10. Requisitos

- Esta política de seguridad se establece y será desarrollada aplicando los siguientes requisitos:

ENS 01 Marco organizativo [ORG]
ENS 02 Marco operacional [OP]
ENS 03 Medidas de protección [MP]
ENS 05 Política de autorización [PA] (dentro de [ORG])
Política de Seguridad del SGSI GuardedBox – ORG.1
Normativa de Seguridad del SGSI GuardedBox – ORG.2
Procedimientos de Seguridad del SGSI GuardedBox – ORG.3
Política de Autorización del SGSI GuardedBox – ORG.4
Planificación del SGSI GuardedBox – OP.PL
Control de Acceso del SGSI GuardedBox – OP.ACC
Explotación del SGSI GuardedBox – OP.EXP
Servicios Externos del SGSI GuardedBox – OP.EXT
Continuidad del Servicio del SGSI GuardedBox – OP.CONT
Monitorización del SGSI GuardedBox – OP.MON
Protección de servicios en la nube – OP.NUB
Medidas de Protección del SGSI GuardedBox – MP

11. Marco normativo

Todo lo establecido en la presente Política de Seguridad está en base a las siguientes normas, regulación y legislación vigente:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y su modificación según el Real Decreto 951/2015, de 23 de octubre y según el Real Decreto 311/2022 de 3 de mayo (se tendrá en cuenta el último texto consolidado).
- ISO 27001 Sistemas de Gestión de Seguridad de la Información.
- 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.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la Información y Comercio Electrónico (LSSI).
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- 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.

12. Estructuración, acceso y control de la documentación de seguridad del SGSI

Todo lo relativo a la estructuración, acceso, control y aprobación de la documentación del SGSI se define en el documento de "Procedimiento de control documental" REF.DOC.GBSGSI.MAN.1, que detalla:

- Formato de los documentos, nomenclatura y proceso de creación de contenido.
- Tipología de documentos.
- Proceso de aprobación de documentos.
- Almacenamiento de documentos.
- Política de publicación y distribución de documentos.
- Política de destrucción de documentos.
- Política de actualización de documentos.
- Validez de los documentos.
- Limpieza de documentos.

13. Registros de actividad

GUARDEDBOX 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:

- 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 incluyen 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.
- Asegurar la mejora continua de la seguridad del sistema.
- Garantizar que los servicios de IT mantengan un desempeño óptimo.
- Reducir los posibles riesgos e impactos que pueda causar un potencial 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 excelencia empresarial.

14. Referencias

Las referencias utilizadas a lo largo de este documento pueden encontrarse en el documento [REF.GBSGSI.REF.1].

15. Firma del documento

Por la presente, la Dirección de GUARDEDBOX afirma cumplir con la legislación citada, y asume la responsabilidad final y última del cumplimiento de la política.



Firmado: [Raúl Siles Peláez] Fecha: [27/10/2024]

Cargo: [Director General de GuardedBox S.L.]