Política de Seguridad de la Información

Uso	Realizado por	Aprobado por
INTERNO	RESPONSABLE DE SEGURIDAD	COMITÉ DE SEGURIDAD

Control de revisiones			
Revisión	**Fecha**	**Descripción**	**Fecha aprobación**
00	12/12/2024	Creación de Documento	15/12/2024

Contenidos

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

CODOCTECH , siendo 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, desarrolla los procedimientos adecuados, 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, autenticidad, trazabilidad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la seguridad 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, así como, 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.

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.

Es decir:

Versión Español

"Los sistemas de información que dan soporte a desarrollo, implantación y mantenimiento de aplicativo (CODOC) según la declaración vigente.

Versión Inglés

"The information systems that support the development, implementation, and maintenance of the application (CODOC) in accordance with the current declaration"

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 y resto de partes interesadas, así como la actualización continua de los mismos. Para ello, el marco legal y regulatorio en el que desarrollamos nuestras actividades queda a tal fin relacionado en nuestro listado de requisitos legales en vigor el cual es revisado y actualizado conforme a periodicidad establecida en nuestro sistema de gestión.

Normativa	Descripción
UNE-EN ISO/IEC 27001:2022	Sistemas de Gestión de Seguridade la Información. Requisitos
Real Decreto 311/2022, de 3 de mayo,	Por el que se regula el Esquema Nacional de Seguridad.
Reglamento (UE) 2016/679 del Parlamento Europeo y	Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos
Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016	Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo DOUEL 04-05-2016 119 C. Deroga la Directiva anterior 95/46/CE (Reglamento general de protección de datos).
Ley Orgánica 3/2018, de 5 de diciembre	Protección de Datos Personales y garantía de los derechos digitales.
Real Decreto 1720/2007, de 21 de diciembre	Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
Real Decreto 611/2023, de 11 de julio	Por el que se aprueba el Reglamento del Registro de la Propiedad Intelectual.
Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014	Sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE

Normativa	Descripción
Real Decreto 513/2017, de 22 de mayo	Reglamento de instalaciones de protección contra incendios
Real Decreto-ley 8/2019, de 8 de marzo	Medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo
Real Decreto 902/2020, de 13 de octubre	De igualdad retributiva entre mujeres y hombres
Real Decreto 901/2020, de 13 de octubre	Regula los planes de igualdad y su registro y se modifica el Real Decreto 713/2010, de 28 de mayo, sobre registro y depósito de convenios y acuerdos colectivos de trabajo
Real Decreto-ley 3/2021, de 2 de febrero	Medidas para la reducción de la brecha de género y otras materias en los ámbitos de la Seguridad Social y económico
Ley Orgánica 3/2007, de 22 de marzo	Para la igualdad efectiva de mujeres y hombres
Ley 2/2023, de 20 de febrero,	Reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción
Ley 34/2002	De Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
BOE-A-2023-16215 Real Decreto 611/2023, de 11 de julio	Relativa al plazo de protección del derecho de autor y de determinados derechos afines

Normativa	Descripción
Real Decreto Legislativo 1/1996, de 12 de abril	Texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
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
Ley 31/1995, de 8 de noviembre	Ley de Prevención de Riesgos Laborales
Real Decreto 486/1997, de 14 de abril,	Por el que se establecen las disposiciones mínimas de seguridad y salud en los lugares de
Real Decreto 488/1997, de 14 de abril	Sobre disposiciones mínimas de seguridad y salud relativas al trabajo con equipos que incluyen pantallas de visualización.
Real Decreto 171/2004, de 30 de enero	Por el que se desarrolla el artículo 24 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, en materia de coordinación de actividades empresariales.
Ley 28/2005, de 26 de diciembre	De medidas sanitarias frente al tabaquismo y reguladora de la venta, el suministro, el consumo y la publicidad de los productos del tabaco.
Real Decreto 171/2004, de 30 de enero	Desarrolla el artículo 24 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, en materia de coordinación de actividades empresariales

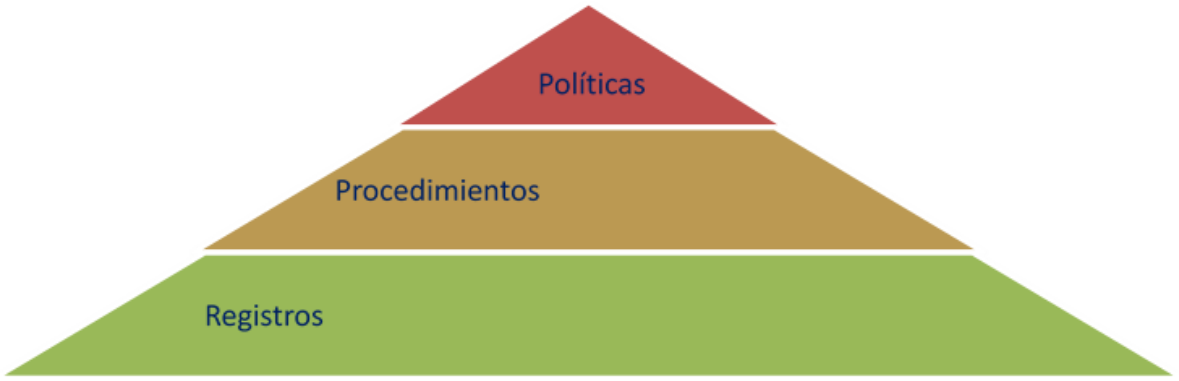
Normativa	Descripción
Ley 40/2015, de 1 de octubre	de Régimen Jurídico del Sector Público
Ley 39/2015, de 1 de octubre,	del Procedimiento Administrativo Común de las Administraciones Públicas.
Real Decreto Legislativo 1/2007, de 16 de noviembre	Texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
Ley 3/2014, de 27 de marzo	Modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre.
RD 475/2007	Clasificación nacional de actividades económicas 2009 CNAE
Contratos con clientes	Condiciones generales y particulares incluidas en los contratos con los clientes

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, 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:



La gestión de nuestro sistema se encomienda al Responsable de Sistemas Informáticos y el sistema estará disponible en nuestro sistema de información en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos.

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 y de la norma UNE-ISO/IEC 27001:2023. 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.

Los roles o funciones de seguridad definidos son:

Función	Deberes y responsabilidades
Responsable de la información	- Tomar las decisiones relativas a la información tratada
Responsable de los servicios	- Coordinar la implantación de los servicios - Mejorar los servicios de forma continua
Responsable de la seguridad	- Determinar la idoneidad de las medidas técnicas - Proporcionar la mejor tecnología para el servicio
Responsable del sistema	- 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	- Implantación, gestión y mantenimiento de las medidas de seguridad

Implantación, gestión y mantenimiento de las medidas de seguridad.

Esta definición de deberes y responsabilidades se completa en los perfiles de puesto y en los documentos del sistema Registro de responsables, roles y responsabilidades.

Resolución de conflictos

Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité del SIG y prevalecerá en todo caso el criterio de la Dirección General.

8. Comité de Seguridad de la Información

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 del Sistema

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.

La organización de la Seguridad de la información se desarrolla en el documento complementario a esta Política de Organización de la Seguridad.

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

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.

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.

10. Gestión de Personal

Todos los miembros de Nuestra Organización 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 TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de Nuestra Organización atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Nuestra 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.

11. Profesionalidad y seguridad de los recursos humanos

Esta Política se aplica a todo el personal de Nuestra Organización 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.

El Responsable de Seguridad, 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 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.

El Responsable de Seguridad participará en la preparación del Compromiso de Confidencialidad que firmarán los empleados y terceros que desempeñen funciones en Nuestra Organización, en el asesoramiento sobre las sanciones que se aplicarán por incumplimiento de esta Política y en el tratamiento de incidentes de seguridad de la información.

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

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.
- Asegurarse 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 nuestra Organización 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. 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 nuestra organización .
- Proteger el equipo de procesamiento de información crítico de Nuestra 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 la misma 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 nuestra 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 nuestra Organización : instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.
- El Responsable de la Seguridad, junto con los Titulares 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 Nuestra Organización a las áreas restringidas bajo su responsabilidad. Los Propietarios de Información autorizará formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de Nuestra Organización cuando lo consideren apropiado.
- Todo el personal de Nuestra 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.

14. 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.

La política de desarrollo y adquisición de sistemas de información se desarrolla en el documento de Política Adquisición, Desarrollo y Mantenimiento de Sistemas.

15. Seguridad por defecto

Nuestra 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.

16. Integridad y actualización del sistema

Nuestra Organización 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.

17. Protección de la información almacenada y en tránsito

Nuestra 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.

18. Prevención de sistemas de información interconectados

Nuestra Organización 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.

19. Registros de actividad

Nuestra 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.

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.

20. Continuidad de la actividad

Nuestra 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.

21. Mejora continua del proceso de seguridad

Nuestra Organización establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en normas internacionales y que se integran en el presente Sistema de Gestión de la Seguridad de la Información.