cegid



Plan de seguridad

CEGID

23/04/2025

www.cegid.com

Acerca de este documento

El objetivo de este documento es presentar el plan de seguridad de Cegid.

Nivel de confidencialidad	Público
Última actualización	23/04/2025

ÍNDICE

Índice 3

1. Cambios del documento 8

2. Introducción 9

2.1. Finalidad del documento 9

2.2. Ámbito de aplicación 9

2.3. Cambios del PS 9

2.4. Definiciones 10

2.5. Documentos de referencia 11

3. Funciones y responsabilidades 12

4. Descripción de los servicios 13

5. Mejores prácticas 14

6. Gestión de riesgos 16

7. Política de seguridad de la información 17

8. Organización de la seguridad de la información 18

8.1. Organización interna 18

8.1.1. Funciones y responsabilidades 18

8.1.2. Separación de tareas y área de responsabilidad 18

8.1.3. Gestión 19

8.1.4. Relación con los organismos y las autoridades 19

8.1.5. Vigilancia y seguridad 19

9. Seguridad vinculada a los recursos humanos 20

9.1. Contratación 20

9.2. Gestión de la confidencialidad 20

9.3. Gestión de la competencia 21

9.3.1. Sensibilización sobre la seguridad 21

9.3.2. Competencia y formación 21

10. Gestión de activos 22
10.1. Inventario 22
10.2. Identificación de los activos 22
10.3. Gestión documental 22
10.4. Gestión de soportes y equipos relacionados con los datos de clientes 22
10.4.1. Almacenamiento 22
10.4.2. Transferencia física 22
10.4.3. Eliminación 22
10.4.4. Mantenimiento 22
10.5. Gestión de activos materiales de los empleados de Cegid 23
10.5.1. Mantenimiento del material 23
10.5.2. Eliminación 23
10.5.3. Gestión de soportes extraíbles 23
10.5.4. Actualización, antivirus y cifrado de soportes 23
11. Política de protección de los sistemas operativos 24
11.1. Sistema operativo de los servidores 24
12. Control de accesos 25
12.1. Política de contraseñas 25
12.1.1. Política para los administradores técnicos de Cegid 25
12.1.2. Política para los clientes de Cegid 25
12.2. Gestión de derechos 26
12.3. Gestión del acceso a los servidores 26
12.4. Supresión de accesos 26
12.5. Revisión de derechos 26
13. Criptografía 27
13.1. Transferencia de datos a redes públicas 27
13.2. Transferencia de datos a otros soportes 27
13.3. Certificados 27
13.4. Cifrado 27

13.5. Movilidad 27

14. Protección física y de entorno 28

14.1. Localización 28

14.2. Centros de datos 28

14.2.1. Seguridad física de los centros y control de accesos 28

14.2.2. Seguridad de los equipos 28

14.3. Instalaciones de Cegid 28

14.3.1. Seguridad de los centros 28

14.3.2. Control de accesos 29

14.3.3. Escritorio limpio 29

15. Seguridad operativa 30

15.1. Datos 30

15.1.1. Clasificación de datos 30

15.1.2. Seguridad de los archivos 30

15.1.3. Seguridad de las bases de datos 30

15.1.4. Cifrado de datos 30

15.1.5. Integridad de los datos 30

15.1.6. Finalización del contrato 30

15.2. Gestión de cambios 31

15.3. Protección contra programas maliciosos 31

15.4. Copias de seguridad 32

15.4.1. Política de copias de seguridad 32

15.4.2. Controles y restauración 32

15.4.3. Principios de conservación 32

15.5. Gestión de información de trazas de auditoría (Logs) 32

15.5.1. Recopilación de información de trazas de auditoría (Logs) 32

15.5.2. Política de acceso a las herramientas 33

15.5.3. Uso de la información de trazas de auditoría (Logs) 33

15.6. Supervisión 33

15.6.1. Principios 33

15.6.2. Equipos de guardia 34

15.7. Gestión de actualizaciones 34

15.7.1. Gestión de los programas instalados 34

15.7.2. Actualización del sistema 34

15.7.3. Actualización de aplicaciones 34

16. Seguridad de las comunicaciones 35
16.1. Arquitectura técnica 35
16.2. Acceso de telecomunicaciones 35
16.2.1. Internet 35
16.2.2. Redes wifi 35
16.3. Equipos de seguridad 35
16.3.1. Cortafuegos 35
16.3.2. IDS/IPS 35
16.3.3. Anti DDoS 36
16.3.4. Alta disponibilidad y tolerancia a fallos 36
17. Adquisición, desarrollo y mantenimiento de los sistemas de información 37
17.1. Ciclo de vida del desarrollo seguro 37
17.2. Segregación de los entornos 37
17.3. Adquisición 38
18. Relación con los proveedores 39
19. Gestión de vulnerabilidades e incidentes relacionados con la seguridad de la información 40
19.1. Gestión de vulnerabilidades 40
19.2. Escaneo de vulnerabilidades 40
19.3. Gestión de incidentes de seguridad 41
19.4. Gestión de crisis 41
20. Gestión de la continuidad de la actividad 42
20.1. Continuidad de la dirección 42
20.2. Plan de continuidad de la actividad y resiliencia 42
20.3. RPO y RTO 42
20.3.1. RPO 42
20.3.2. RTO 42
21. Cumplimiento normativo 43
21.1. Normas y reglamentos 43
21.1.1. ISO 27001 43

21.1.2. RGPD y protección de datos personales 43
21.1.3. Seguridad relativa a la Inteligencia Artificial 43
21.1.4. Auditoría 43
21.1.4.1. Auditoría interna 43
21.1.4.2. Auditoría externa 44
21.1.4.3. Auditoría técnica 44
21.1.4.4. Auditoría de clientes 44

1. CAMBIOS DEL DOCUMENTO

Las fechas que aparecen en la siguiente tabla son las fechas de aprobación del documento.

Fecha	Autor	Tipo de cambio
03/11/2016	Equipo de seguridad de Cegid	Versión inicial
02/02/2018	Equipo de seguridad de Cegid	Revisión del documento
30/07/2018	Equipo de seguridad de Cegid	Revisión del documento
23/05/2019	Equipo de seguridad de Cegid	Revisión del documento
07/10/2020	Equipo de seguridad de Cegid	Revisión del documento
08/08/2022	Equipo de seguridad de Cegid	Fusión de los planes de seguridad existentes dentro del de Cegid
03/04/2023	Equipo de seguridad de Cegid	Revisión del Documento, se añaden las ofertas relevantes en el alcance y corrección de errores tipográficos
04/03/2024	Equipo de seguridad de Cegid	Revisión del Documento, se añaden las ofertas relevantes en el alcance y corrección de errores tipográficos
06/06/2024	Equipo de seguridad de Cegid	Se añaden las ofertas relevantes en el alcance
23/04/2025	Equipo de seguridad de Cegid	Revisión del Documento, se añaden las ofertas relevantes en el alcance y corrección de errores tipográficos. Cambios por transición de ISO27001:2013 a versión 2022

2. INTRODUCCIÓN

2.1. Finalidad del documento

El presente documento constituye el plan de seguridad (PS) y puede adjuntarse a los contratos de los clientes. Describe los compromisos asumidos por Cegid para satisfacer los requisitos contractuales de seguridad de los sistemas de información (SI) previstos para:

- Proteger los recursos de los SI utilizados para realizar las actividades y presentar los entregables previstos en el contrato.
- Proteger al cliente de los daños que podría sufrir debido a la indisponibilidad de estos recursos o la violación de su integridad o su confidencialidad.

Este plan de seguridad recoge las disposiciones de seguridad relativas a las medidas físicas, organizativas, procedimentales y técnicas aplicadas.

Las medidas descritas en este documento pueden ser complementadas con aquellas descritas en el libro de servicio correspondiente a cada oferta de Cegid.

2.2. Ámbito de aplicación

Este documento se aplica a los servicios SaaS prestados por los equipos de Cegid Cloud y a las actividades de estos equipos.

2.3. Cambios del PS

Cualquier cambio del PS dará lugar a una nueva versión del presente documento. Las modificaciones se registran con la fecha correspondiente en el historial de versiones al inicio del documento.

Una modificación secundaria[1] no dará lugar necesariamente a una nueva versión inmediata del PS. Esta modificación aparecerá en la próxima versión del documento.

Cualquier cambio del PS formará parte del mismo de manera obligatoria y vinculará igualmente a las partes.

En caso de modificación del documento, prevalecerá la versión publicada en el sitio web oficial de Cegid. La versión adjunta al contrato del cliente permite verificar que no haya ninguna regresión.

El PS se revisa al menos una vez al año. Esta revisión puede originar la edición de una nueva versión del presente documento.

---

1 Modificación que no afecta a los requisitos de seguridad.

2.4. Definiciones

Activos: Conjunto de bienes o prestaciones de servicios que permiten proporcionar las ofertas de Cegid.

ASVS : Application Security Verification Standard

BSIMM: Building Security In Maturity Model

CAB: Change Advisory Board (Junta asesora de cambios)

Cliente: Cliente de una solución contemplada en este documento.

CMP: Cloud Management Platform (Plataforma de gestión en la nube)

DPO: Data Privacy Officer (Delegado de protección de datos)

GED: Gestión electrónica de documentos

IPS: Sistema de prevención de intrusiones

ITSM: Information Technology Service Management (Gestión de los servicios de tecnología de la información)

Pliego del servicio: Documento que describe las condiciones particulares de cada oferta SaaS de Cegid.

Cegid Cloud: Organización dentro de Cegid encargada del diseño, el funcionamiento y el soporte técnico de la plataforma SaaS de Cegid (véase Presentación de Cegid Cloud).

ISO: International Standard Organization (Organización Internacional de Normalización)

OWASP: Open Web Application Security Project

PS: Plan de seguridad

PAM: Privileged Access Management (Gestión de accesos con privilegios)

PSSI: Política de seguridad de los sistemas de información

RGPD: Reglamento General de Protección de Datos

RPO: Recovery Point Objective o Punto objetivo de recuperación

RSSI: Responsable de la seguridad de los sistemas de información

RTO: Recovery Time Objective o Tiempo bjetivo de recuperación

SAMM : Software Assurance Maturity Model

SGSI: Sistema de gestión de la seguridad de la información. Este término designa un conjunto de políticas relativas a la gestión de la seguridad de la información.

Términos del Servicio: Documento que describe las condiciones específicas para cada oferta de Cegid.

VM: Virtual Machine (Máquina virtual)

VPN: Red privada virtual

2.5. Documentos de referencia

CGU: Condiciones generales de uso de los servicios de Cegid. Están disponibles en www.cegid.com, el sitio web de Cegid.

ISO 27001:2022: Norma para los sistemas de gestión de seguridad de la información

ISO 27002:2022: Guía de mejores prácticas para los SGSI

ISO 27005:2018: Norma para la gestión de riesgos de seguridad de la información

Términos del servicio: Documentos que describen las condiciones particulares de cada oferta SaaS de Cegid. Están disponibles en www.cegid.com, el sitio web de Cegid.

3. FUNCIONES Y RESPONSABILIDADES

Cegid se apoya en las infraestructuras de sus socios para prestar sus servicios. La instalación y el mantenimiento de estas infraestructuras corren a cargo de sus socios.

4. DESCRIPCIÓN DE LOS SERVICIOS

Los servicios específicos de las aplicaciones de Cegid y su descripción se presentan en los pliegos de servicios.

5. MEJORES PRÁCTICAS

La Seguridad de Cegid está gestionada por un equipo centralizado que se guía por el estándar de seguridad ISO27001 para todo el Grupo. Cegid está certificado en ISO27001:2022 para las siguientes áreas:

- "Servicio para alojar aplicaciones que contengan datos facilitados por los clientes en un entorno de nube".
  Certificado n.º IS 666376 expedido por BSI
  Centros de Francia: Lyon (69), Vénissieux (69), Boulogne Billancourt (92) y Nantes (44)
  Servicios Cegid SaaS en el alcance de esta certificación: Cegid Expert, Cegid Fiscalité (ex-Your Cegid Fiscalité), Cegid HR (Suite Ex-Talentsoft), Cegid HR Sprint, Cegid Loop, Cegid Notilus (Modules Notes de frais et Déplacements), Cegid Optitaxes, Cegid Payroll Ultimate (ex Cegid HR Ultimate), Cegid Portail Etafi, Cegid PMI, Cegid Quadra (ex-Cegid Quadra Expert), Cegid Quadra Entreprise Plus, Cegid Retail, Cegid RHP, Cegid RHPi, Cegid Tax Flex, Cegid Tax Ultimate, Cegid XRP Flex, Cegid XRP Sprint.

- "Desarrollo y explotación de software de Pagos y Gestion de Cash en modo SaaS"
  Certificado n.º 2023/106509.3 expedido por AFNOR
  Centro de Francia: Boulogne Billancourt (92)
  Servicios Cegid SaaS en el alcance de esta certificación: Cegid Exabanque, Cegid Allmybanks, Cegid MesBanques, Cegid Direct-Debits.

- "Servicios SaaS RR.HH. y Nómina y Gestión del Tiempo de Visualtime prestados en diferentes modelos de servicio para facilitar la gestión de los recursos humanos a los clientes de Cegid Spain".
  Certificado n.º IS 589848 expedido por BSI
  Centro de España: Madrid y Barcelona
  Servicios Cegid SaaS en el alcance de esta certificación: Cegid Peoplenet HR, Cegid Peoplenet Payroll y Cegid VisualTime en España

- "Servicio para alojar aplicaciones de gestión y desarrollo de los recursos humanos que contengan datos facilitados por los clientes en un entorno de nube".
  Certificado n.º CA09/77186 expedido por SGS
  Centro de Canadá: Montreal
  Centro de EE. UU.: Nueva York
  Centro de Francia: París (75)
  Servicios Cegid SaaS en el alcance de esta certificación: Cegid Talent

- "Diseño, entrega, y soporte continuo de la aplicación StorIQ"
  Certificado n°20/3244 expedido por CfA
  Centro de Reino Unido: Londres
  Servicios Cegid SaaS en el alcance de esta certificación: Cegid Retail Store Excellence

- "El sistema de gestión de la seguridad de la información que da soporte a las actividades de instalación, mantenimiento y soporte del servicio de alojamiento Cloud de las aplicaciones de los clientes de Ekon Cloud Computing Solutions SAU, según la Declaración de Aplicabilidad, versión APL 001/21."
  Certificado n.º: ES 122286-1 expedido por Bureau Veritas
  Centro de España: Barcelona
  Servicios Cegid SaaS en el alcance de esta certificación: Cegid Ekon, Cegid XRP Enterprise

  - Informe ISAE 3402 Type II para Cegid Tax Ultimate (solo para Francia)

  - Informe ISAE 3402 Type II para Cegid Allmybanks

  - Informe ISAE 3000 Type I como Payment Service Provider (PSP) para clientes de Swift Alliance Lite 2 (SAL2)

  - SWIFT Customer Security Controls Framework (CSCF) para Cegid Allmybanks

  - Informe SOC1 Tipo II para Peoplenet Nómina (Argentina y Mexico)

  - Informe SOC2 Tipo II para Peoplenet Nómina (Spain, Portugal, Argentina, Mexico, Colombia and Chile)

  - Informe SOC1 Tipo II report on Cegid HR (suite Talentsoft, módulo Career)

  - Informe ISAE 3402 Tipo II para PeopleNet Nómina France

  - Certification Customer Security Program (CSP) Swift para Cegid Treasury basado en el CSCF

Los siguientes servicios Cegid SaaS están cubiertos por este Plan de Seguridad aunque no estén en el alcance de ninguna de las certificaciones mencionadas anteriormente: Cegid Assurex, Cegid HR (Module Talent Acquisition Ex-Digitalrecruiters), Cegid ISIE, Cegid Orli, Cegid Payroll Peoplenet en Francia y en LATAM, Cegid Peoplenet Dedicated, Cegid Peoplenet Enterprise, Cegid Retail UR, Cegid XRP Ultimate, Cegid Treasury.

Si no puedes localizar tu producto en las listas no dudes en contactar con nuestro departamento comercial para obtener más información.

El objetivo es proteger las funciones y la información de pérdidas, robos o alteraciones, así como los sistemas informáticos de intrusiones o daños.

Respetar un ciclo de vida del desarrollo de software seguro permite garantizar la seguridad en las aplicaciones alojadas. Este ciclo de vida se basa en los principios de los marcos de control de referencia OWASP SAMM, BSIMM y OWASP ASVS.

6. GESTIÓN DE RIESGOS

El proceso de evaluación de riesgos del Grupo incluye la identificación, el análisis y la gestión de los riesgos del modelo empresarial y las entidades usuarias.

Cegid reconoce que la gestión de riesgos es una parte fundamental de sus actividades. La dirección ha creado un mapa de riesgos para Cegid Cloud en cuatro ámbitos:

Tipos de riesgos:

- Riesgos asociados a los recursos humanos
- Riesgos estratégicos
- Riesgos informáticos
- Otros riesgos

Este proceso permite a la dirección de Cegid comprender y hacer un seguimiento de los riesgos pertinentes que podrían afectar a la empresa y aplicar medidas para mitigarlos.

Además, se realizan análisis de riesgos específicos de los diferentes SGSI basados en los principios de la norma ISO 27005 y métodos reconocidos internacionalmente (EBIOS 2010, EBIOS RM, MAGERIT).

El análisis de riesgos forma parte de la seguridad de los SI de Cegid. Se ejecuta de forma continua entre los equipos de operaciones y los equipos de seguridad.

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Las actividades de Cegid se rigen por políticas de seguridad de la información. Estas políticas se introdujeron en 2008 y se revisan todos los años. Se basan en los principios y las mejores prácticas de las normas ISO 27001:2022 e ISO 27002:2022.

La finalidad de estas políticas es proteger la información crítica de Cegid, de sus clientes y de sus socios.

Las políticas se comunican a las personas interesadas. Con el fin de proteger al máximo la seguridad y la integridad de sus plataformas, Cegid no divulga los nombres ni los datos de los elementos de seguridad aplicados (proveedores, empresas de software, etc.).

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

8.1. Organización interna

8.1.1. Funciones y responsabilidades

Se han definido y atribuido las responsabilidades en materia de seguridad.

Se nombra a un RSSI para todas las actividades de Cegid. Esta persona es responsable de un equipo dedicado a la seguridad.

Los equipos implicados en la seguridad de la información son:



8.1.2. Separación de tareas y área de responsabilidad

Para limitar el riesgo de modificación o alteración de los activos (no autorizada o involuntaria), se separan las tareas y las áreas de responsabilidad de los equipos.

En particular, todas las actividades de alojamiento para nuestros clientes están separadas del resto de entornos de la empresa, tanto a nivel organizativo como a nivel técnico.

Asimismo, dentro de las actividades de alojamiento para nuestros clientes, se aplica un principio de separación de tareas a través de la gestión de derechos vinculados a las necesidades de las actividades.

Una organización matricial del Grupo permite definir las áreas de responsabilidad por actividad, especialmente aquellas relacionadas con la responsabilidad de la seguridad de los datos de clientes, activos y riesgos, que permiten prestar los servicios de Cloud.

8.1.3. Gestión

Existen órganos directivos a nivel estratégico y a nivel operativo con comités específicos.

Estos órganos se reúnen con regularidad para hacer un seguimiento de temas relacionados con la seguridad de los sistemas de información. Las actas se guardan en el sistema de gestión documental.

8.1.4. Relación con los organismos y las autoridades

Cegid es miembro de asociaciones profesionales (CLUSIF (Club francés de la seguridad de la información), CESIN (Club francés de expertos en seguridad de la información y tecnología digital), Incibe (Instituto Nacional de Ciberseguridad de España), Club ISO27001, etc.). Cegid mantiene relaciones con las autoridades (ANSSI [Agencia francesa de seguridad de los sistemas de información], CNIL [Comisión francesa de informática y libertades], CCN-Cert [Centro Criptológico Nacional], AEPD [Agencia Española de Protección de Datos], CERT-MX [Centro de Respuesta a Incidentes Cibernéticos de México], etc.) para seguir los avances en el ámbito de la seguridad de la información.

8.1.5. Vigilancia y seguridad

Cegid ha establecido una estrategia de vigilancia de la seguridad, a nivel técnico y legal. Permite prevenir los riesgos vinculados específicamente a las actividades de Cegid.

Cegid cuenta además con los servicios CERT de empresas especializadas en vigilancia de la seguridad para incrementar su capacidad de búsqueda. Este método de búsquedas múltiples permite cotejar la información encontrada y obtener resultados adaptados y pertinentes en el contexto de la actividad de Cegid.

9. SEGURIDAD VINCULADA A LOS RECURSOS HUMANOS

9.1. Contratación

La información de los candidatos se verifica de conformidad con los reglamentos, las normas éticas, las leyes y cualquier legislación relevante en vigor en la jurisdicción pertinente. Estas verificaciones son proporcionales a las exigencias del puesto, la clasificación de la información accesible y los riesgos identificados.

Entre las verificaciones establecidas, se encuentran:

- Verificación del currículum del candidato.
- Verificación de las competencias relacionadas con el puesto.
- Copias de los diplomas, cursos y cualificaciones profesionales mencionadas en el currículum.
- Control de identidad independiente, pasaporte o documento de identidad.
- Verificación de la validez del permiso de trabajo o del permiso de residencia si se trata de un candidato extranjero.

9.2. Gestión de la confidencialidad

Los siguientes aspectos están contemplados en los contratos, el reglamento interno y las normas de uso de los sistemas informáticos:

- Respeto de la propiedad intelectual.
- Respeto de la legislación sobre la protección de los datos personales.
- Protección de la información, los activos vinculados a la información y las aplicaciones de la empresa y sus clientes.
- Protección de la información procedente de socios, otras organizaciones y terceros.

Pueden aplicarse disposiciones particulares en las siguientes situaciones:

- Inicio de un proceso disciplinario formal y público contra los empleados que infrinjan las normas de seguridad de la información. Constituye un elemento disuasorio para que los empleados no infrinjan las políticas y los procedimientos relativos a la seguridad de la empresa, así como cualquier otra norma de seguridad.
- Responsabilidades estipuladas en el contrato de trabajo que siguen siendo de aplicación durante un periodo determinado tras finalizar el contrato.

Todos los empleados están obligados por contrato a respetar la confidencialidad. Este compromiso de confidencialidad se aplica a todos los datos facilitados por los clientes a través de documentos o en reuniones.

9.3. Gestión de la competencia

9.3.1. Sensibilización sobre la seguridad

Los nuevos empleados deben seguir un programa de inducción que incluye una fase de sensibilización sobre la seguridad y la confidencialidad.

El plan de sensibilización y una serie de instrumentos específicos permiten hacer un seguimiento regular de temas sensibles relacionados con la seguridad (campaña de *phishing*, Safe Desk, etc.).

9.3.2. Competencia y formación

Cada año los empleados de Cegid y sus superiores celebran entrevistas de desempeño y objetivos con el fin de mantener el conocimiento requerido, identificar necesidades de formación y organizar el intercambio de conocimientos. Durante estas entrevistas, se discute sobre los planes de formación necesarios. Los responsables de RR. HH. elaboran un plan de formación anual a partir de estas necesidades y de la estrategia de la empresa.

10. GESTIÓN DE ACTIVOS

10.1. Inventario

Cegid crea inventarios de los activos esenciales y los activos secundarios. Estos figuran en los análisis de riesgos para poder centralizar los riesgos asociados.

Cuando sea técnicamente posible y pertinente, un proceso automatizado de actualización permite sincronizar el inventario y los activos presentes en el entorno SaaS.

10.2. Identificación de los activos

La identificación de los activos usados en la prestación de los servicios de Cegid se basa en convenciones de nomenclatura formalizadas. En la mayoría de los casos, y cuando resulte relevante, estas convenciones de nomenclatura no permiten establecer un vínculo directo con los clientes.

10.3. Gestión documental

Cegid cuenta con sistemas de gestión documental que tienen en cuenta los procesos y los procedimientos necesarios para el funcionamiento de los servicios prestados a los clientes.

10.4. Gestión de soportes y equipos relacionados con los datos de clientes

10.4.1. Almacenamiento

Los soportes extraíbles que contienen datos de clientes se almacenan en un lugar seguro cuando no están en uso.

Los soportes no extraíbles que contienen datos de clientes están alojados en centros de datos.

10.4.2. Transferencia física

A la hora de transferir físicamente un soporte con datos que no sean de dominio público, Cegid utiliza exclusivamente transportistas reconocidos y de confianza que proponen un seguimiento y justificantes de entrega. En caso de que Cegid deba devolver datos en un soporte transmitido por un cliente, lo hará con las mismas técnicas y los mismos medios empleados para su envío.

10.4.3. Eliminación

La eliminación de los activos está sujeta a un procedimiento particular de eliminación de datos confidenciales. Este procedimiento impone una eliminación segura o una destrucción física de los soportes que hayan contenido datos confidenciales.

10.4.4. Mantenimiento

La responsabilidad de los equipos hardware que contienen los datos de clientes corresponde a los proveedores de infraestructura de Cegid.

10.5. Gestión de activos materiales de los empleados de Cegid

10.5.1. Mantenimiento del material

La DSI de Cegid proporciona los equipos a los empleados de Cegid. La DSI y sus proveedores se encargan del mantenimiento de estos dispositivos. Se mantiene un inventario de la asignación de estos equipos y los empleados son responsables de su seguridad física.

10.5.2. Eliminación

Los soportes de almacenamiento presentes en los equipos eliminados se destruyen de forma segura según los procedimientos aplicables (software de borrado de datos, eliminación de claves de cifrado de discos, etc.).

10.5.3. Gestión de soportes extraíbles

Se aplica una política de seguridad de los soportes extraíbles administrada por los empleados de los equipos de Cegid Cloud. Esta política se implementa a través de un software de tipo Endpoint o de GPO que no permiten limitar el uso de soportes extraíbles.

10.5.4. Actualización, antivirus y cifrado de soportes

La DSI se encarga de las actualizaciones del sistema y las aplicaciones de Cegid (ofimática, aplicaciones internas, etc.), la actualización de la protección contra programas maliciosos y el cifrado de los soportes (internos y extraíbles). Se crean regularmente indicadores que el equipo de seguridad analiza.

11. POLÍTICA DE PROTECCIÓN DE LOS SISTEMAS OPERATIVOS

Se implementa una política de bastionado seguro para proteger los sistemas operativos. Consiste en reducir la superficie de ataque posible desactivando o suprimiendo los objetos (servicios, aplicaciones, funcionalidades, etc.) que no sean esenciales. Esto se consigue aplicando opciones de seguridad particulares y actualizando los programas informáticos.

11.1. Sistema operativo de los servidores

Las operaciones de bastionado en los sistemas operativos de los servidores se aplican a:

- Actualizaciones
- Estrategia de cuenta
- Derechos de los usuarios y red
- Registro
- Protección contra programas maliciosos
- Funciones y funcionalidades
- Espacio de usuario
- Espacio de disco

Estas operaciones se basan en las guías del CIS, la ANSSI y el NIST.

12. CONTROL DE ACCESOS

12.1. Política de contraseñas

Cada usuario de Cegid cuenta con un nombre de usuario único y una contraseña segura.

Las contraseñas de los usuarios no se almacenan abiertamente en el sistema de información de Cegid.

La norma por defecto para nuestros sistemas es utilizar funciones de cifrado irreversibles de tipo «hash» con algoritmos seguros.

En el caso de los sistemas AS400, se usa un cifrado de Vigenère con una clave X-OR.

12.1.1. Política para los administradores técnicos de Cegid

La gestión de las contraseñas de los administradores técnicos de Cegid está sujeta a una política de seguridad estricta:

- Longitud mínima: 10 caracteres.
- Complejidad: letras en mayúsculas y minúsculas, cifra y símbolo
- Frecuencia de cambio: cada 60 días
- Imposibilidad de reutilizar las últimas 24 contraseñas
- Bloqueo tras 5 intentos (desbloqueo por parte de un administrador de Cegid)

Esta política de seguridad se ve reforzada para ciertos grupos como los administradores de Cegid Cloud.

12.1.2. Política para los clientes de Cegid

La política estándar de contraseñas para los usuarios de los clientes de Cegid es la siguiente:

- Longitud mínima: 8 caracteres
- Complejidad: letras en mayúsculas y minúsculas, cifra y símbolo
- Frecuencia de cambio: cada 90 días
- Imposibilidad de reutilizar las 24 últimas contraseñas
- Bloqueo tras 5 intentos (desbloqueo por parte de un administrador de Cegid o el usuario a través de una herramienta de gestión en línea de contraseñas)

Algunas aplicaciones permiten delegar la gestión de las credenciales al cliente. Cuando se activa esta federación de identidades, el cliente tiene libertad para gestionar y aplicar su propia política de contraseñas. Cegid recomienda a sus clientes utilizar esta opción respetando siempre las exigencias del RGPD.

12.2. Gestión de derechos

La gestión de derechos para los equipos de Cegid se basa en el principio de privilegio mínimo. Cada equipo posee los derechos necesarios únicamente para la actividad que desempeña.

Controles periódicos de los accesos se realizan por parte del Equipo de Seguridad.

Las solicitudes de derechos (adición, modificación, supresión, etc.) a las principales aplicaciones y ámbitos se envían a través de flujos de trabajo.

Por razones de confidencialidad, no se divulgará ningún dato personal de los empleados de Cegid.

12.3. Gestión del acceso a los servidores

Únicamente las personas con las autorizaciones necesarias pueden acceder a los servidores que contienen datos de clientes. Cegid cuenta con directorios específicos de los sistemas de producción independientes del SI interno.

12.4. Supresión de accesos

La supresión de accesos para el personal de Cegid está vinculada al proceso de RR. HH. de gestión de salidas o de movilidad interna. Estas acciones se supervisan a través de herramientas de flujos de trabajo internos.

En cuanto a los empleados externos, las modificaciones o la supresión de derechos son responsabilidad de su superior.

12.5. Revisión de derechos

El equipo de seguridad organiza la revisión de los derechos de los principales entornos y aplicaciones. Los accesos se revisan periódicamente sobre la base de un análisis de riesgos.

13. CRIPTOGRAFÍA

13.1. Transferencia de datos a redes públicas

Los datos se encriptan al transferirlos a redes públicas con protocolos seguros (HTTPS, TLS, SFTP, SSH, etc.).

13.2. Transferencia de datos a otros soportes

En el caso de soportes extraíbles (p. ej.: memorias o unidades USB), el cliente debe encriptar los soportes antes de enviarlos a Cegid, si es necesario con la ayuda de los equipos de soporte técnico. De no hacerlo, el cliente será responsable de la seguridad de sus datos durante el transporte y la recepción por parte de Cegid. Después de integrar los datos, los soportes se borran antes de devolverlos al cliente.

13.3. Certificados

Con el fin de garantizar el más alto nivel de seguridad, los certificados HTTPS usados por Cegid proceden de autoridades de certificaciones públicas y reconocidas. La gestión de estos certificados se rige por procedimientos que tienen en cuenta su ciclo de vida.

13.4. Cifrado

Las normas sobre la longitud de las claves de cifrado son las siguientes:

- Cifrado asimétrico: superior o igual a 2048 bits
- Cifrado simétrico: superior o igual a 256 bits

Cegid utiliza programas de cifrado basados en el estándar AES256 para crear archivos seguros.

En relación con la encriptación, los protocolos de comunicación para nuestros sitios externos utilizan al menos TLS 1.2.

13.5. Movilidad

Los equipos de administración de Cegid utilizan únicamente sus ordenadores portátiles para conectarse a distancia.

14. PROTECCIÓN FÍSICA Y DE ENTORNO

14.1. Localización

Los centros de datos utilizados por Cegid están repartidos por todo el mundo para poder responder a las exigencias reglamentarias de los clientes. Cegid se asegura de que sus proveedores cumplen las normas técnicas y de seguridad. Los centros de datos se eligen antes de la fase de producción y en función de las ofertas de Cegid.

14.2. Centros de datos

14.2.1. Seguridad física de los centros y control de accesos

Con el fin de ofrecer un nivel óptimo de seguridad, todos los centros de datos utilizados por Cegid cuentan con la certificación ISO 27001. Únicamente las personas autorizadas pueden visitar los centros de datos.

14.2.2. Seguridad de los equipos

Se han adoptado una serie de medidas y principios en el diseño de la infraestructura para garantizar un nivel óptimo de disponibilidad e integridad de los servicios de Cegid.

La norma principal consiste en evitar cualquier punto de fallo único (*single point of failure* en inglés) en los equipos o los enlaces.

Por ejemplo:

- Redundancia a nivel de los servicios físicos
- Redundancia a nivel de la red
- A nivel del almacenamiento
- Virtualización

14.3. Instalaciones de Cegid

14.3.1. Seguridad de los centros

Las instalaciones de Cegid están sujetas a las mismas normas que el resto de las instalaciones de Cegid Lyon Vaise, principalmente:

- Suministro de energía con contrato individual + sistema de alimentación ininterrumpida.
- Detectores de incendios y extintores.
- Suministro de servicios de aire acondicionado, calefacción y ventilación.

14.3.2. Control de accesos

El acceso a las instalaciones está protegido con lectores de tarjetas. Cada empleado cuenta con una tarjeta programada que le permite acceder total o parcialmente a determinadas zonas del edificio.

Los controles de accesos físicos forman parte de la gestión de derechos descrita en el párrafo 12.2.

14.3.3. Escritorio limpio

Se aplica una política de escritorio limpio en las instalaciones de los equipos de Cegid. Los documentos, equipos o cualquier otro soporte que pueda contener información confidencial deben estar guardados cuando no se utilicen.

15. SEGURIDAD OPERATIVA

15.1. Datos

15.1.1. Clasificación de datos

La norma ISO 27001 exige una clasificación de los activos y datos esenciales. Esta clasificación se establece en al menos tres niveles:

- Público
- Limitado
- Confidencial

En este contexto, los datos de clientes están clasificados como «confidenciales».

15.1.2. Seguridad de los archivos

Los archivos de datos se almacenan en directorios específicos para cada uno de nuestros clientes. Estos directorios están protegidos con los mecanismos de seguridad facilitados por los sistemas operativos subyacentes.

Esto permite garantizar la seguridad, la compartimentación y el hermetismo entre cada cliente.

15.1.3. Seguridad de las bases de datos

Cegid utiliza para sus bases de datos sistemas estándar y conocidos de tipo Microsoft SQL, Oracle, MySQL, MongoDB, DB2, etc.

Al seleccionar a las principales empresas del sector, Cegid puede contar con fabricantes de software experimentados y con una comunidad activa para mantener siempre sus sistemas de gestión de bases de datos a un nivel óptimo.

15.1.4. Cifrado de datos

Las transferencias de datos entre el puesto de trabajo de los clientes y el SI de Cegid se protegen con protocolos de cifrado descritos en 13.1.

15.1.5. Integridad de los datos

Cegid se compromete a aplicar procedimientos, medidas técnicas y protocolos seguros para transmitir y conservar los datos de sus clientes con el fin de protegerlos de posibles alteraciones (voluntarias o accidentales).

15.1.6. Finalización del contrato

Las condiciones de conservación y supresión de los datos de los clientes tras la finalización de un contrato se detallan en los documentos contractuales.

15.2. Gestión de cambios

Los cambios siguen el procedimiento a continuación:

Cambios de aplicaciones:

- Se autorizan los cambios estándar y normales previa validación de un comité. Por ejemplo, entre estos cambios, se encuentran: las actualizaciones de portales estándar, las actualizaciones de fiscalidad, los cambios de configuración, las correcciones de errores y vulnerabilidades, etc.

Cambios de infraestructuras y sistemas:

- Autorizados previa validación de un comité: cambios de infraestructura que afecten directamente a la producción, resolución de incidentes, gestión de capacidades y seguridad.
- Autorizados sin la validación de un comité: intervenciones corrientes para mantener la producción en condiciones operativas.

Periodos especiales:

- En función de la estacionalidad de los productos y las actividades de nuestros clientes, los cambios están restringidos en determinados periodos, generalmente conocidos como «periodos de congelación».

Cambios URGENTES:

- Los cambios urgentes deben aplicarse rápidamente y no pueden esperar el próximo ciclo de validación.
- Esta categoría de cambio está reservada para la resolución de una crisis o un riesgo crítico inminente (p. ej. fallo de seguridad, incidente grave, etc.).
- Esta categoría de cambio se estudia en un comité reunido de urgencia (p. ej. eCAB/Emergency CAB).

15.3. Protección contra programas maliciosos

Todas las infraestructuras del servidor están protegidas con soluciones antivirus y antimalware centralizadas. Los servidores centrales (Hub) controlan al menos una vez al día la existencia de actualizaciones de los fabricantes. A continuación, se difunden por todos los servidores.

El control de antivirus está integrado en la supervisión del SI de Cegid y está sujeto a indicadores que se revisan en comités relacionados con la seguridad de la información.

15.4. Copias de seguridad

15.4.1. Política de copias de seguridad

Los datos de los clientes son una prioridad para los equipos de Cegid. Con el objetivo de garantizar la integridad y la disponibilidad de los datos, Cegid cuenta con un eficaz sistema de copias de seguridad.

El principio que aplica Cegid es el de la doble copia de seguridad:

- Una primera copia se realiza en los sistemas de producción en una primera infraestructura de uso exclusivo.
- A continuación, se duplica en una segunda infraestructura de uso exclusivo.

Las infraestructuras de copias de seguridad no están ubicadas en el mismo centro de datos que los sistemas de producción. Esta organización garantiza un nivel óptimo de disponibilidad e integridad al tiempo que satisface nuestras exigencias de RTO y RPO (véase el capítulo 20.3).

La frecuencia de las copias de seguridad y el periodo de conservación varían según las ofertas y se detallan en el pliego de la oferta en cuestión.

15.4.2. Controles y restauración

Las herramientas de monitorización y reporte realizan un control de las tareas de copia de seguridad. En caso de producirse un incidente durante una copia de seguridad, se emite automáticamente una alerta que procesarán los equipos de Cegid.

Como parte de sus operaciones periódicas, Cegid hace restauraciones cada día. Estas permiten validar el buen funcionamiento de las copias de seguridad, así como los procesos de restauración asociados.

15.4.3. Principios de conservación

Como empresa de software especializada, Cegid conoce las actividades y las necesidades de sus clientes. Esta característica ha permitido instaurar periodos de conservación de copias de seguridad específicos para cada oferta propuesta.

Los principios de conservación se detallan en el pliego de cada oferta.

15.5. Gestión de información de trazas de auditoría (Logs)

15.5.1. Recopilación de información de trazas de auditoría (Logs)

Una serie de herramientas de concentración y correlación de registros de eventos (logs) permite mantener la trazabilidad en el SI de Cegid. Estos registros se conservan con fines técnicos y

operativos durante un periodo adaptado en función de las obligaciones legales, contractuales y operativas.

Estas herramientas permiten uniformizar el periodo de conservación de los datos recopilados y garantizar su seguridad.

Los datos recopilados son, por ejemplo, el nombre de usuario, su hora de conexión y desconexión, la aplicación utilizada, la dirección IP de origen, etc.

Los equipos de Cegid pueden acceder a los registros, que no pueden exportarse para el cliente. Estos registros podrán transmitirse al cliente únicamente en casos justificados, como la resolución de un incidente. Algunas ofertas de Cegid proponen registros de aplicaciones disponibles directamente en la aplicación.

15.5.2. Política de acceso a las herramientas

Los empleados de Cegid Cloud pueden acceder a las herramientas para garantizar el funcionamiento de la plataforma, con derechos adaptados a sus funciones (véase el capítulo 12).

15.5.3. Uso de la información de trazas de auditoría (Logs)

Ejemplos de usos de la información recopilada:

- Responder a las obligaciones reglamentarias y contractuales vinculadas a las actividades de Cegid.
- Hacer un seguimiento del estado de los sistemas gestionados por Cegid Cloud y poder detectar lo antes posible cualquier evento que pueda perjudicar al servicio.
- Producir datos estadísticos anonimizados sobre la prestación del servicio.

El uso de estadísticas y datos procedentes de la información de los logs de auditoría se rige por las condiciones generales de uso.

15.6. Supervisión

15.6.1. Principios

Se supervisan todos los servicios y sistemas gestionados por Cegid Cloud. Las herramientas de supervisión utilizan el protocolo SNMP o bien sistemas automáticos desarrollados específicamente para recuperar los datos procedentes de todos los puntos de control.

Una sala de vigilancia remota permite a los equipos de Cegid Cloud hacer un seguimiento permanente del estado de determinados servicios. Se emiten alertas en tiempo real en caso de fallo de los servicios supervisados.

Las herramientas están vinculadas a sistemas que envían SMS a los equipos de guardia durante las horas no laborables.

15.6.2. Equipos de guardia

Los equipos de guardia se encargan de supervisar e intervenir en el SI de Cegid las 24 horas del día todos los días de la semana. Están compuestos por especialistas que representan todos los ámbitos de competencia de Cegid.

15.7. Gestión de actualizaciones

15.7.1. Gestión de los programas instalados

Cegid utiliza un conjunto de programas que permiten inventariar y controlar todos los programas presentes en el SI, así como en los puestos de administración.

15.7.2. Actualización del sistema

Los sistemas se actualizan a través de consolas centralizadas.

El principio que sigue Cegid para realizar actualizaciones tanto críticas como de seguridad es el siguiente: las actualizaciones se aplican a lo largo de un ciclo mensual en un conjunto de entornos de pruebas al salir un parche para garantizar que no da problemas de integridad o disponibilidad del servicio prestado a los clientes. Si no se detecta ningún problema, se extenderá a toda la plataforma de producción.

En caso de indisponibilidad de un parche, se usará una solución alternativa para no afectar a la seguridad del servicio propuesto.

15.7.3. Actualización de aplicaciones

Cegid cuenta con un sistema de gestión de los cambios industrializado (véase el capítulo 15.2) que permite gestionar las actualizaciones de aplicaciones según los compromisos definidos en los términos de servicio de sus soluciones SaaS.

16. SEGURIDAD DE LAS COMUNICACIONES

16.1. Arquitectura técnica

La infraestructura que da soporte a los servicios de Cegid está compartimentada y organizada en zonas de seguridad y zonas de aplicaciones. Este principio permite ofrecer un alto nivel de seguridad adaptado a las necesidades actuales y futuras.

16.2. Acceso de telecomunicaciones

16.2.1. Internet

Cegid tiene sus propias direcciones IP públicas y varios puntos de acceso a internet de diferentes proveedores para poder prestar a sus clientes el nivel de servicio esperado en caso de fallo de uno de los proveedores.

Todas las comunicaciones ofrecidas por Cegid están protegidas y utilizan los protocolos mencionados en el capítulo 13.1

16.2.2. Redes wifi

Las redes wifi están compartimentadas según su función (wifi para invitados, empleados, móvil, etc.) y su acceso depende de la gestión de derechos. Los puntos de acceso wifi están protegidos.

En los centros de datos, la red wifi está prohibida.

16.3. Equipos de seguridad

16.3.1. Cortafuegos

Existen cortafuegos entre cada zona de seguridad y cada zona de aplicaciones.

Los flujos procedentes del exterior atraviesan varias capas de cortafuegos antes de llegar al servicio solicitado.

Los flujos directos hacia las zonas de confianza no están autorizados. Deben pasar obligatoriamente por las zonas desmilitarizadas (DMZ).

16.3.2. IDS/IPS

Se han instalado dispositivos IDS/IPS en determinadas localizaciones estratégicas de las redes para analizar los flujos entrantes y salientes del SI de Cegid. Su función es detectar los flujos anormales y el tráfico malicioso, y bloquearlos.

Los dispositivos descargan las actualizaciones de firmas de ataque de expertos en seguridad del fabricante de software y se despliegan bajo la responsabilidad del equipo de seguridad de Cegid.

Estos datos se correlacionan en paneles de control e indicadores.

16.3.3. Anti DDoS

Todas las plataformas e infraestructuras se benefician de una protección anti DDoS adaptada a las distintas tecnologías aplicadas.

16.3.4. Alta disponibilidad y tolerancia a fallos

La disponibilidad de los servicios de Cegid está garantizada gracias a la redundancia de los sistemas para responder a una avería, el fallo de un componente o una indisponibilidad temporal. Entre las tecnologías utilizadas, destacan:

- Virtualización de los servidores.
- Redundancia del almacenamiento de datos.
- Equilibrio de carga en clústeres en los equipos de redes y telecomunicaciones.
- Método de *capacity planning* con extensión en caliente (VM y cortafuegos).
- Equilibrio de carga de aplicaciones en las granjas de servidores.

17. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

La seguridad del desarrollo es una cuestión primordial para Cegid.

Cegid ha adoptado una estrategia para integrar la seguridad durante todo el ciclo de vida de las aplicaciones desarrolladas. Esta estrategia se basa en las recomendaciones de OWASP SAMM, OWASP ASVS y BSIMM.

17.1. Ciclo de vida del desarrollo seguro

Un equipo de gobierno agrupa las actividades relacionadas con la organización del ciclo de vida del desarrollo seguro con la definición de políticas, objetivos de medición y un programa de formación y sensibilización asociado.

Un equipo de diseño agrupa las actividades relacionadas con la recopilación de exigencias de seguridad, las especificaciones de arquitectura de alto nivel y el diseño detallado.

Un equipo de implementación agrupa las actividades y los procesos de construcción e instalación de los componentes de los programas (véase el capítulo 15.2), así como aquellas relacionadas con la gestión de fallos.

Un equipo de verificación agrupa las actividades relacionadas con las pruebas de funcionamiento correcto, de no regresión y de seguridad que permiten garantizar la calidad de los programas desarrollados.

En su conjunto, el objetivo de la estrategia es mejorar la calidad y la seguridad de los productos entregados con, entre otros:

- Una comunidad de desarrolladores de referencia en el ámbito de la seguridad dentro de cada equipo de desarrollo.
- Herramientas para revisar la seguridad del código.
- Un repositorio común (OWASP) que permite aprovechar información sobre seguridad, así como difundir y aplicar las mejores prácticas.
- Un sistema de vigilancia de la seguridad específico con boletines de información, actualizaciones y mejoras enviados a los equipos.

17.2. Segregación de los entornos

Las redes y las infraestructuras de Cegid están separados de forma física y lógica según los servicios.

Asimismo, la plataforma aplica una separación de los diferentes entornos de aplicaciones (desarrollo, pruebas, preproducción y producción). El entorno de desarrollo está exclusivamente reservado y disponible para los desarrolladores y no contiene ningún dato de producción salvo acuerdo particular por contrato con el cliente.

Se puede acceder a los equipos a través de un bastión administrativo o máquina virtual de rebote (Jumphost) para los equipos con privilegios necesarios.

17.3. Adquisición

Al adquirir nuevos sistemas, se tienen en cuenta las necesidades de seguridad en el proceso de selección.

18. RELACIÓN CON LOS PROVEEDORES

Con el fin de elaborar una política coherente con sus actividades, Cegid clasifica sus proveedores en función de su carácter crítico con respecto a la prestación de los servicios a los clientes. En función de su carácter crítico, se prevén diferentes controles, por ejemplo:

- Análisis de sus certificaciones de seguridad.
- Creación de comités de seguimiento de la seguridad con indicadores de eficacia y cumplimiento.
- Auditorías técnicas y organizativas.
- Creación y seguimiento de SLAs de seguridad.
- Creación de cláusulas de seguridad específicas en los contratos.
- Clasificación de funciones y responsabilidades en la gestión de incidentes de seguridad.

Para poder prestar sus servicios, Cegid utiliza infraestructuras proporcionadas por sus proveedores. Es responsabilidad de estos proveedores el despliegue y mantenimiento de dichas infraestructuras.

19. GESTIÓN DE VULNERABILIDADES E INCIDENTES RELACIONADOS CON LA SEGURIDAD DE LA INFORMACIÓN

19.1. Gestión de vulnerabilidades

Las vulnerabilidades se clasifican según el sistema CVSS V3.0 y se procesan por defecto de acuerdo con la tabla siguiente:

Tipo de vulnerabilidad	Puntuación CVSS	Compromiso del plan de acción
Low	0,1 – 3,9	Best Effort
Medium	4,0 – 6,9	Best Effort
High	7,0 – 8,9	7 días tras la detección
Critical	9,0 – 10	7 días tras la detección

En el caso de algunos productos o servicios, los planes de acción pueden iniciarse más tarde según se indica en los términos de servicios.

19.2. Escaneo de vulnerabilidades

Se ejecutan escaneos periódicos en todo el perímetro de internet del SI de Cegid, y al menos una vez al mes, a través de un escaneo de vulnerabilidades gestionado por el equipo de seguridad de Cegid.

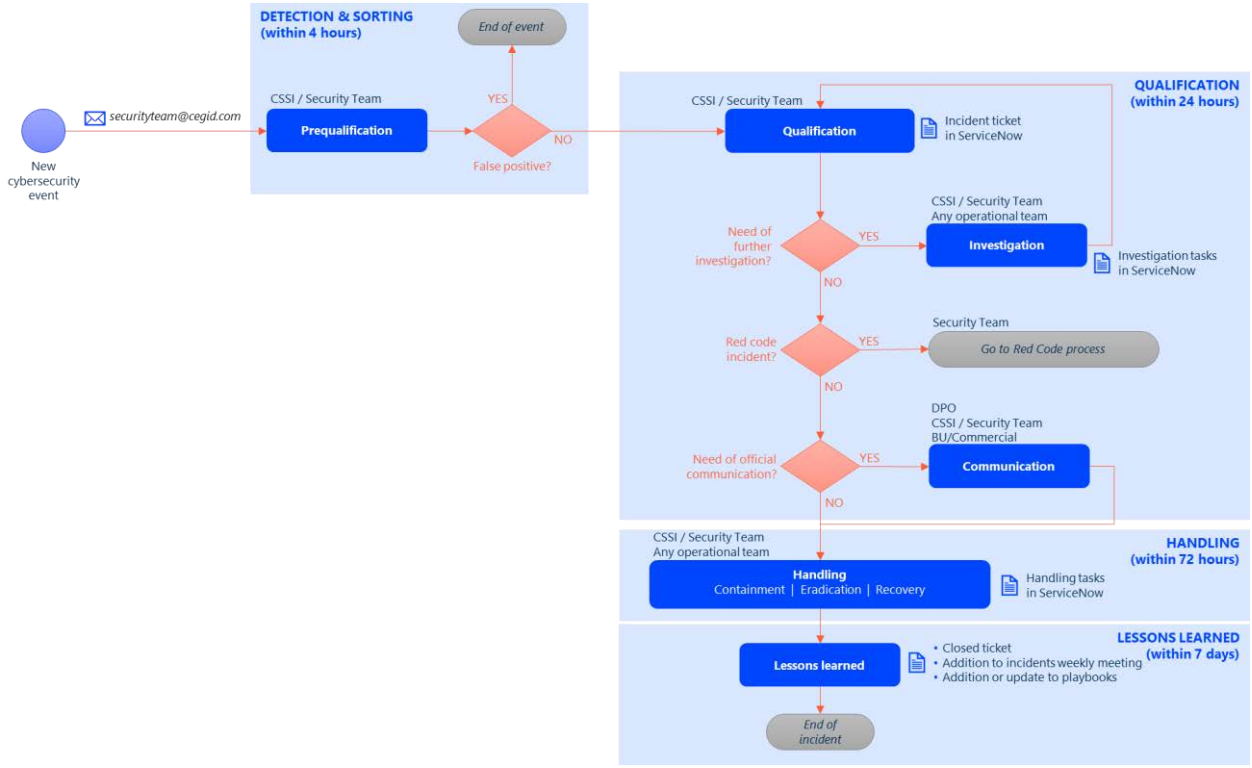
Estos escaneos permiten controlar la configuración correcta de los equipos y programas con el fin de detectar vulnerabilidades.

Los resultados se revisan y dan lugar a planes de acción específicos.

19.3. Gestión de incidentes de seguridad

Un flujo de trabajo procesa los incidentes de seguridad en las herramientas ITSM de Cegid. El principio se basa en las mejores prácticas presentes en las normas ISO 27001 e ISO 27002.

Se establece del siguiente modo:



Se comunica el incidente a los clientes o socios implicados en un plazo máximo de 72 horas tras evaluar el sistema afectado.

En función del tipo de plan de acción, Cegid puede también ponerse en contacto con las entidades relevantes de Cegid para organizar la resolución del incidente.

19.4. Gestión de crisis

Se formalizan planes de gestión de crisis específicos, incluyendo escenarios de crisis gobernados por una organización y procesos completamente definidos. Se mantienen actualizados directorios de gestión de crisis para mejorar la coordinación de las acciones requeridas ante una situación de crisis. Estas medidas también garantizan una respuesta estructurada a situaciones de crisis en Cegid.

20. GESTIÓN DE LA CONTINUIDAD DE LA ACTIVIDAD

20.1. Continuidad de la dirección

Se ha definido un plan de continuidad para la gestión y la dirección de los servicios (infraestructura, aplicaciones, etc.) para los equipos de Cegid.

La continuidad de estas actividades se basa a la vez en la creación de arquitecturas resilientes de los sistemas de control y en la seguridad de los ordenadores portátiles que permite a cualquier empleado o administrador de los equipos de Cegid acceder, de forma segura, a distancia y de conformidad con los derechos concedidos, a los recursos y herramientas que permiten prestar el servicio.

20.2. Plan de continuidad de la actividad y resiliencia

La continuidad de la actividad se tiene en cuenta por defecto desde la fase de diseño de los servicios prestados por Cegid.

El plan de continuidad de la actividad (BCP) se define de forma global e incluye una dimensión humana, organizativa y técnica. Se adapta a cada una de las ofertas en función de las limitaciones de las actividades y las arquitecturas técnicas.

Los recursos críticos (recursos humanos, infraestructuras, sistemas de información y recursos inmateriales) se identifican para cada oferta.

El BCP se diseña para responder a las necesidades de continuidad expresadas para la disponibilidad de los servicios.

Más allá del diseño de la resiliencia de las arquitecturas técnicas y de software, los procesos operativos y organizativos del BCP se definen y se prueban en un modo de mejora continua.

20.3. RPO y RTO

20.3.1. RPO

RPO: Recovery Point Objective o Punto Objetivo de Recuperación

El RPO figura en los términoss de servicios. Por defecto, son 24 horas.

20.3.2. RTO

RTO: Recovery Time Objective o Tiempo Objetivo de Recuperación

Generalmente, Cegid no define RTO en los términos de servicios, pero, en el caso de determinadas ofertas particulares, se garantiza un RTO (véase el contrato o el término del servicio).

En caso de que un siniestro grave provoque una interrupción prolongada del servicio, Cegid se compromete a restaurar cuanto antes el servicio a partir de la copia de seguridad más adecuada.

21. CUMPLIMIENTO NORMATIVO

21.1. Normas y reglamentos

21.1.1. ISO 27001

Los equipos de Cegid se rigen por la norma ISO 27001:2013 para diseñar y prestar los servicios a los clientes. Las certificaciones y ámbitos cubiertos se enumeran en el capítulo 5.

Con el fin de proponer una arquitectura y una infraestructura en línea con los conocimientos técnicos existentes en materia de seguridad, Cegid cuenta con centros de datos y servicios asociados con la certificación ISO 27001.

21.1.2. RGPD y protección de datos personales

Cegid ha adoptado una política de confidencialidad y cookies disponible en su sitio web: https://www.cegid.com/es/privacy-policy/

21.1.3. Seguridad relativa a la Inteligencia Artificial

La Inteligencia Artificial está siendo integrada de forma nativa en varias aplicaciones de Cegid siguiendo la estrategia de la compañía para los próximos años.

En Cegid, damos prioridad a la seguridad e integridad de nuestras implementaciones de IA, garantizando que cumplan con los más altos estándares de seguridad y cumplimiento. En consonancia con la Ley de Inteligencia Artificial de la Unión Europea (EU AI Act https://artificialintelligenceact.eu/the-act/) publicada el 12 de julio de 2024, hemos adoptado un marco riguroso para integrar las tecnologías de IA de forma responsable y segura en nuestras aplicaciones. Nuestro compromiso se ve reforzado por nuestra participación activa en el Pacto por la IA (https://digital-strategy.ec.europa.eu/en/policies/ai-pact#ecl-inpage-Signatories-of-the-AI-Pact), a través del cual nos comprometemos a respetar las mejores prácticas y directrices éticas en el despliegue de la IA. Esto incluye la realización de evaluaciones de riesgos exhaustivas, la aplicación de medidas sólidas de protección de datos y la supervisión continua de los sistemas de IA para protegerlos de las vulnerabilidades.

21.1.4. Auditoría

21.1.4.1. Auditoría interna

El control de las actividades de seguridad en los ámbitos de certificación de Cegid corre a cargo de consultores cualificados bajo la supervisión del departamento de seguridad.

En un intervalo planificado, revisan los elementos relacionados con los ámbitos certificados de conformidad con el plan de auditoría de Cegid.

Los documentos sobre las auditorías internas son confidenciales y no pueden divulgarse. En el caso de un incumplimiento que suponga un riesgo para la seguridad, Cegid se compromete a ponerse en contacto con los clientes impactados en el alcance afectado (véase § Gestión de incidentes y seguridad).

21.1.4.2. Auditoría externa

En el marco de las certificaciones ISO 27001:2013 listadas en la Sección 5 de este documento los organismos certificados auditan Cegid anualmente para el alcance de dichas certificaciones.

21.1.4.3. Auditoría técnica

Asimismo, Cegid encarga a expertos cualificados auditorías técnicas periódicas de su SI.

La planificación periódica de estas auditorías técnicas permite probar cada aplicación estratégica en un ciclo de 3 años.

21.1.4.4. Auditoría de clientes

Los clientes suscriptores pueden hacer pruebas de penetración en los servicios que utilizan en las condiciones indicadas en el contrato.

Las auditorías de organización pueden también organizarse a iniciativa de los clientes. Están sujetas a determinadas condiciones de elegibilidad y requieren la firma de cláusulas contractuales particulares.