POLÍTICA GENERAL DE SEGURIDAD

CONTROL DEL DOCUMENTO

Información básica del documento	
Tipo	Política
Nombre del documento	Política General de Seguridad/ Política del SGSI
Versión	V 6.0
Autor	Silvia Mª Canut
Nombre del fichero	CI SG1 5.2 – Política General SGSI
Organización interna	QTSP – POLITICAS
Fecha de creación	20 de Enero 2021
Estado	Aprobado
Fecha de aprobación	30 de Diciembre 2021

Historial del documento		
Versión	Fecha	Cambios
V.1	19/05/15	**Creación y publicación.** POLITICA DE SEGURIDAD. Coloriuris establece un marco para la fijación de objetivos relacionados con la seguridad de la información. También se establecen unos objetivos de seguridad de la información y unos requisitos para el correcto ejercicio de la actividad ante los clientes y dentro de la organización interna.
V.2	15/09/16	**Cambios y publicación.** REVISIÓN EXTRAORDINARIA. - Se añade el apartado ‘’Comunicación a terceras partes’’. - Se establece un procedimiento de notificación de incidencias de seguridad en Coloriuris. - Ante las incidencias acaecidas, se establecerán notificaciones internas, externas y ante organismos públicos. - En caso de cambios en la política de seguridad las comunicaciones serán solamente externas o ante los correspondientes organismos.
V.3	30/06/17	**Cambios y publicación.** REVISIÓN EXTRAORDINARIA. - Cambios de estilo - Cambios en la redacción - Incorporación de información general más detallada.
V.4.1	12/12/17	**Cambios y publicación**. REVISIÓN ORDINARIA. Procedimiento de revisión de la política de seguridad ante posibles cambios legislativos o en la normativa ISO/IEC 27001 que sean de aplicación a Coloriuris. - Se procede a añadir quién es el responsable de las revisiones ordinarias, el contenido que debe ser examinado, y su adecuada notificación.
V.4.2	19/07/18	**Revisión y publicación.** REVISIÓN ORDINARIA. - No hay cambios. Se mantiene la versión.
V.4.3	22/07/19	**Revisión y publicación.** REVISIÓN ORDINARIA. - No hay cambios. Se mantiene la versión.

V.5	16/10/19	**Cambios y publicación.** REVISIÓN EXTRAORDINARIA. A raíz de la auditoría eIDAS de 2019, y para dar cumplimiento a lo estipulado en la observación #4 del CAR: ‘’La política de seguridad del prestador define la existencia de requisitos de seguridad, particularmente a efectos de confidencialidad, que son aplicables a los terceros implicados en la prestación de los servicios. No obstante, no se concretan cuáles son dichos requisitos ni se precisa cómo se valorará su efectiva implementación por el prestador. Evidencia: Política de Seguridad de la Información del prestador’’. - Se añade el apartado ‘’Proveedores de Coloriuris’’ dentro del epígrafe ‘’Requisitos de la actividad’’, donde se especifican las obligaciones que asumen los proveedores de Coloriuris respecto del SGSI. - Cambios de estilo y redacción
V.5.1	25/05/20	**Cambios y publicación.** REVISIÓN EXTRAORDINARIA. - Revisión del documento. - Cambios de estilo y maquetación. - Se añade campo de contenido/indice.
V.6	31/12/21	**Cambios y publicación.** REVISIÓN ORDINARIA. - Añadir todo lo relacionado con normativa de Esquema Nacional de Seguridad (ENS) - .

COMITÉ DE SEGURIDAD	Elabora	Firma
	RESPONSABLE DE SEGURIDAD Silvia Mª Canut	CANUT GRAVALOS SILVIA MARIA - 73426574V 31/03/2022 13:57:02 CEST Lugar: 185.75.202.217
	Aprueba	Firma
	RESPONSABLE DEL SERVICIO/Admin de la C.A Javier Teixidó Gaibar	TEIXIDO GAIBAR JAVIER - 73203720X 04/04/2022 17:30:37 CEST Lugar: 82.213.220.90
	RESPONSABLE DE SISTEMAS Cesar Laso Laso	LASO LASO CESAR - 72980225Y 04/04/2022 17:02:13 CEST Lugar: 88.5.231.150
	RESPONSABLE DE LA INFORMACIÓN/ DIRECCIÓN Pedro J. Canut	CANUT ZAZURCA PEDRO JAIME - 73193046P 05/04/2022 08:02:53 CEST Lugar: 185.75.201.195

CONTENIDO

1. REVISIÓN, APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información es efectiva desde la fecha de su **aprobación por el Comité de Seguridad**, hasta que sea reemplazada por una nueva Política.

La presente política se revisará, como mínimo, **cada 12 meses**, es decir, un año natural en CI SGI 9.3_Revisión por dirección que se celebra todos los años en el mes de diciembre, si bien se puede revisar de forma previa, dicha revisión anual se llevará a cabo mediante un proceso de revisión ordinaria, debiendo decidirse, de forma expresa y cada vez que se revise, si se aplica algún cambio a la presente política o si por el contrario se mantiene sin modificaciones hasta la siguiente revisión.
Si en dicha revisión ordinaria no se aplicara ningún cambio, se documentará para que conste este hecho en el informe de revisión por dirección.

También se revisará cada vez que se detecte una posibilidad de mejora o necesidad de cambio en el presente documento, o bien algún cambio a nivel legislativo o normativo en las normas ISO/UNE de aplicación (teniendo en cuenta especialmente la ISO/IEC 27001), Esquema Nacional de Seguridad, ISO 14001 o bien después de pasar una Auditoría en la que el equipo auditor haga alguna recomendación al respecto. Estas revisiones recibirán el nombre de revisiones extraordinarias ya que no están planificadas en el tiempo. Tras detectar un cambio de cualquier índole, o dar respuesta a una necesidad, las modificaciones preceptivas en la presente política se llevarán a cabo de forma inmediata. Cada vez que se vayan a realizar modificaciones o revisiones sobre el presente documento, se levantará un acta en la que se especifiquen los cambios realizados y deberá ser posteriormente firmada por el Comité de Seguridad para su efectiva aprobación.

Las revisiones ordinarias y extraordinarias de la presente política correrán a cargo del **Responsable de Seguridad.** El procedimiento a seguir para detectar posibles cambios legislativos o normativos será el de examinar con relativa frecuencia las páginas web de los organismos oficiales competentes, que contengan los documentos objeto de interés, a fin de comprobar si ha habido cambios que precisen una modificación de las mismas.

2. INTRODUCCIÓN

Coloriuris, S.L es una empresa especializada en prestar servicios relacionados con la seguridad jurídica en la utilización de Internet, entre los cuales se encuentra la acreditación del momento en el que se realiza un acto o transacción. Con esta finalidad la empresa ha creado la "Autoridad de Sellado de Tiempo de Coloriuris S.L." (TSACI).

Las actividades de Coloriuris, S.L. (de aquí en adelante, '**COLORIURIS**'), dependen de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a posibles amenazas (daños accidentales o deliberados) que puedan afectar a la Disponibilidad, Integridad, Confidencialidad, Autenticidad, o Trazabilidad de la seguridad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes, antes de que los daños sean irreparables o inasumibles.
Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la Disponibilidad, Integridad, Confidencialidad, Autenticidad, Trazabilidad, 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.

La política de seguridad, consecuencia de la estrategia adoptada por la Dirección de COLORIURIS para la protección de la Información, tiene como objetivo la implantación de un Sistema de Gestión para la Seguridad de la Información (SGSI) y la Certificación de este, esto implica que se deben aplicar las medidas de seguridad exigidas en conformidad con los requisitos establecidos a través de la Norma Internacional ISO-27001, Esquema Nacional de Seguridad, Ley Orgánica de Protección de Datos y Reglamento Europeo de Protección de Datos, 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.

COLORIURIS debe cerciorarse de que la seguridad de la información 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.

Es por ello, que la Dirección de COLORIURIS pretende con ello alcanzar un alto nivel de calidad en la gestión de sus actividades, y al tiempo ofrecer una imagen consistente con sus servicios de prestador cualificado de servicios de confianza. Para ello proveerá los medios humanos, técnicos y económicos pertinentes, preocupándose de lograr la implicación activa de todos los empleados de la empresa.

Se considera que la seguridad de la información constituye una de sus principales preocupaciones, y que debe estar fundamentada en una dinámica de mejora continua que debe difundirse por toda la organización mediante la adecuada formación, motivación y aumento de la competencia profesional.

De este modo COLORIURIS debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Esquema Nacional de Seguridad y a la Ley Orgánica de Protección de Datos.

Esta Política de Seguridad sigue las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

2.1- Prevención

COLORIURIS debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se implementarán las medidas necesarias de seguridad determinadas por el ENS, ISO-27001, RGPD y la LOPD y GDD 03/2018, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Se considera imprescindible la implicación real de todo el personal de la empresa en la implantación, el mantenimiento, la supervisión y la mejora continua del SGSI. Además, todos y cada uno de los empleados deberán asumir la responsabilidad que les corresponde en función de su actividad dentro de la organización.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados en CI SGI 5.3_Organización de la seguridad.

Para garantizar el cumplimiento de la política, COLORIURIS debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente (AUDITORIAS).

2.2 - Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua, para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

Estas motorizaciones son parte de los INFORMES que se hacen de forma periódica (cada 30 días), se encuentran en la carpeta:

- *REGISTRO-EVIDENCIAS ▫ **INFORMES***

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya preestablecido como normales.

2.3 - Respuesta

COLORIURIS cuenta con procedimientos establecidos de notificación y gestión de incidencias de seguridad, además de establecer canales de comunicación (internos y externos) para tal fin, se encuentran en la carpeta:

- *INCIDENCIAS Y QUEJAS ▫ CI SG1 A 16 Notificación y gestión de Incidencias.*

Es por ello que COLORIURIS se compromete a:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Departamentos o en otros organismos.
- Establecer protocolos de intercambio de información relacionada con incidentes con clientes y proveedores.

2.4 - Recuperación

Para garantizar la disponibilidad de los servicios críticos, COLORIURIS ha desarrollado planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

- *COLORIURIS ▫ CI SG1 5.2 Plan de contingencias y continuidad de negocio*

3. MISIÓN

COLORIURIS define la presente Política de Seguridad de la Información, de carácter obligatorio para empleados y empresas colaboradoras, teniendo como objetivo fundamental garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a los incidentes que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve a COLORIURIS para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

✔ **Disponibilidad:** propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.

✔ **Integridad:** propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.

✔ **Confidencialidad:** propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.

✔ **Autenticidad:** propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.

✔ **Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la información en COLORIURIS quedará determinada por los siguientes elementos:

- Velar por la seguridad de la información, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar y mantener los planes de contingencias y continuidad de la actividad.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información.

- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente:
  - Requisitos legales sobre garantías y derechos de las personas físicas.
  - Legislación vigente sobre la información y su tratamiento.
  - Requisitos contractuales y reglamentos suscritos con clientes y proveedores.
  - Normativa derivada de la implantación y mantenimiento de la norma ISO 27001 y Esquema Nacional de Seguridad.
- Proteger toda información propiedad de la organización, además de los recursos materiales y tecnológicos utilizados para tratar información.

Se tendrán en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y el tratamiento de riesgos.

Además se le dará importancia a los principios que rigen esta Política de Seguridad:

- **Liderazgo:** la Dirección es la piedra angular del sistema de gestión.
- **Participación:** son partícipes todos los empleados y las partes interesadas.
- **Enfoque a procesos:** permite identificar los activos de información.
- **Gestión del riesgo:** su metodología posibilita la aplicación de criterios.
- **Capacitación:** conocer y ejercer de forma competente las responsabilidades.
- **Mejora continua:** su aplicación asegura el progreso del sistema de gestión.

Está Política de Seguridad:

- Se aprobará formalmente por el comité de seguridad.

- Se revisará regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia (todos los años en revisión por dirección).

- Se comunicará a todos los empleados y empresas externas qué trabajen con COLORIURIS.

4. ALCANCE

La Política de Seguridad se aplica a toda la empresa y a sus activos dentro de:

> ***"Los sistemas que dan soporte a: La Gestión de ciclos de vida de los certificados digitales (emisión, validación, mantenimiento y revocación), sellado de tiempo (timestamping) y servicios cualificados de confianza"***

A todos los departamentos dentro de COLORIURIS, tanto a sus directivos como a empleados.

- A los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la organización.
- A bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.
- A la información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas.
- A la información cedida dentro de un marco legal establecido, que será considerada como propia a efectos exclusivos de su protección.
- A todos los sistemas utilizados para administrar y gestionar la información, sean propios o alquilados o licenciados por la misma.

5. DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de COLORIURIS.

- En COLORIURIS se reconoce expresamente la importancia de la información, así como la necesidad de su protección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad de la Institución, o al menos suponer daños muy importantes, si se produjera una pérdida total e irreversible de determinados datos.
- COLORIURIS implementa, mantiene y realiza un seguimiento del Esquema Nacional de Seguridad, ISO-27001, ISO-14001, del RGPD y de la Ley Orgánica de Protección de Datos, y cumple con todos los requisitos legales aplicables.
- La información y los servicios están protegidos contra pérdidas de Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Los controles serán proporcionales a la criticidad de los activos a proteger y a su clasificación.
- La responsabilidad de la seguridad de la información involucrada en la prestación de los servicios incluidos en el alcance del ENS 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 punto 7 “Organización de la Seguridad” de este mismo documento se describen las funciones y responsabilidades del Comité de Seguridad, que gestionará la seguridad de la información, y de sus miembros.
- Quienes desempeñen la función de Seguridad de la Información y otras de administración relacionadas, serán quienes administren la seguridad.
- Se ha identificado a los responsables de la información, que deberán promover el establecimiento de los controles y medidas destinadas a proteger los datos que la integran, especialmente los de carácter personal o críticos.

- Se establecerá dentro de la normativa un sistema de clasificación de la información, con diferentes niveles:
  - Nivel Medio ▫ Web COLORIURIS (publico).
  - Nivel Alto ▫ Organización COLORIURIS (privado).

- Se establecerán los medios necesarios y adecuados para la protección de personas, datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información, y, en general, de cualquier activo de COLORIURIS.
- Los aspectos específicos más relacionados con la información sobre datos personales están regulados por el conjunto de normas recogidas en el documento de *Normativa Aplicable a CI (CI SGI A 18.1.1)*.
- Quienes no cumplan lo determinado en estas normas y en los procedimientos complementarios podrán ser sancionados de acuerdo con la legislación del Estatuto de los trabajadores, o bien con sanciones personalizadas si incumplen con lo que especifica el documento de *Funciones y Obligaciones del Personal de COLORIURIS (CI SG1 7.3)*.
- Deberán realizarse periódicamente evaluaciones de riesgos y, en función de las debilidades, determinar si es necesario elaborar planes de implantación o reforzamiento de controles.
- Se fomentará la difusión de información y formación en seguridad a empleados y colaboradores, previniendo la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar su posible existencia lo antes posible, y en caso de que existieren, procurándose una difusión muy restringida de las indagaciones.
- El personal de COLORIURIS 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.
- Las incidencias de seguridad serán comunicadas y tratadas apropiadamente.

6. MARCO NORMATIVO

COLORIURIS cumple con la legislación que le es de aplicación y con todos sus requerimientos respecto a las recomendaciones internaciones, legislación y normativa, en especial en materia de Seguridad que nos es de aplicación. Corresponde al Responsable de Seguridad de COLORIURIS, que se encargará de tenerla actualizada, con las últimas versiones disponibles, últimas modificaciones y derogaciones documentadas.

Según la legislación vigente, las leyes aplicables a COLORIURIS se encuentran especificadas en el documento:

- COLORIURIS ▫ Normativa ▫ **CI SG1 A 18.1.1 Normativa Aplicable a CI.**

Se irán haciendo revisiones periódicas por parte del Responsable de Seguridad, con la frecuencia suficiente para poder comprobar que no hay nueva normativa que añadir, ni tampoco nuevas versiones de aquella que ya figuraba en el documento. Para ello, se revisarán habitualmente las principales páginas web que contienen el tipo de información que buscamos: www.boe.es , www.etsi.org, www.eurlex. europa.eu , http://www.mineco.gob.es , etc.

7. ORGANIZACIÓN DE LA SEGURIDAD DE COLORIURIS

7.1 - Comité de seguridad: Funciones y Responsabilidades

El Comité de Seguridad tiene como obligación coordinar la seguridad de la información en COLORIURIS.

El **Comité de Seguridad** reportará a la organización y estará formado por:

RESPONSABLE DE SEGURIDAD
RESPONSABLE DEL SERVICIO /Admin del sistema de Certificación
RESPONSABLE DE SISTEMAS
RESPONSABLE DE LA INFORMACIÓN/ DIRECCIÓN

El **Secretario del Comité de Seguridad** será el Responsable de Seguridad y tendrá las funciones:

- Convoca las reuniones del Comité de Seguridad y prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Responsabilizarse de que se elaboren las actas de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

Algunas de las **funciones del Comité de Seguridad** de la Información que debe llevar a cabo son las siguientes:

- Formular, revisar y aprobar la política de Seguridad de la Información.
- Identificar las metas que se persigue con la seguridad de la información y asegurar que éstas estén relacionadas con las exigencias de la organización e integradas en los procesos relevantes.
- Proveer al equipo de directrices claras y de un gran apoyo durante la gestión de iniciativas en materia de seguridad.
- Informar regularmente del estado de la seguridad de la información a la Dirección.

- Facilitar todos los recursos que sean necesarios.
- Llevar a cabo los controles necesarios que verifiquen la idoneidad de la implementación de la Seguridad de la Información que se está realizando en la organización.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

Para mas detalle sobre el Comité de Seguridad de COLORIURIS acudir a:

- EQUIPO ▫ ROLES DE SEGURIDAD ▫ **CI SG1 5.3 Organización de la Seguridad CI.**

7.2- Roles: Funciones y Responsabilidades

En el caso de COLORIURIS todas las responsabilidades recaen en el Director General/Dirección, al ser una Sociedad Limitada con varios socios y un Administrador único.

Algunas de las funciones y responsabilidades se nombran a continuación:

Responsable de Seguridad

- Mantener la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad.
- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
- Gestionar la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.

- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.

Responsable del Servicio / Admin. de la C.A (*Autoridad de Certificación*)

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.
- Responsable de la generación de los certificados raíz, certificados de la TSA y certificado de firma del OCSP.
- Autorizado para realizar cambios en la configuración del sistema de certificación.
- Responsable de implementar, configurar, mantener, monitorizar, documentar y asegurar el correcto funcionamiento del sistema de certificación.
- El Responsable de Sistemas de Certificación garantiza el tiempo de actividad, rendimiento, uso de recursos y la seguridad del HSM que gestiona.

Responsable de la información

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.

Responsable de Sistemas

- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.

- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Responsable de la gestión del día a día del sistema (monitorización, backup, recovery…).
- El Responsable de Sistemas de Certificación garantiza el tiempo de actividad, rendimiento, uso de recursos y la seguridad de los servidores que administra de forma dinámica.

Dirección

- Se encuentra dentro del Comité de Seguridad de la Información de Coloriuris.
- Coordina al Comité de Seguridad de la Información de Coloriuris.
- Facilita los recursos que sean necesarios para la implantación de medidas de SGSI.
- Autoriza aquellos documentos que deban ser revisados antes de su puesta en marcha.
- Supervisa las actividades relacionadas con el tratamiento de datos.
- Impulsa medidas de mejora continua respecto al SGSI.

Para más información de las funciones y responsabilidades de los diferentes roles de COLORIURIS en función de la normativa acudir a:

- EQUIPO ▫ ROLES DE SEGURIDAD ▫ **CI SG1 5.3 Organización de la Seguridad CI.**

8. PROCEDIMIENTO DE DESIGNACIÓN

El procedimiento de Designación/Nombramiento en COLORIURIS se detalla a continuación.

La Dirección nombra:

- ✔ **Responsable de Seguridad**, que reportará al Comité de Seguridad.
- ✔ **Responsable del Servicio**, que reportará al Comité de Seguridad.
- ✔ **Responsable de la Información,** que reportará al Comité de Seguridad.
- ✔ **Responsable de Sistemas,** que reportará al Comité de Seguridad.
- ✔ **Administrador de C.A,** que reportará al Comité de Seguridad.

Está designación queda reflejada en el documento de Responsabilidades y Procedimientos (CI SG1 A 16.1.1) y/o Organización de la Seguridad CI (CI SG1 5.3) , que está en la carpeta EQUIPO

- ▫ Roles de Seguridad/Liderazgo.

Por lo tanto, cada vez que cambie de persona, Dirección y el nuevo responsable firmará el documento .

9. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad la revisión periódica (de forma anual) de esta Política General de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Comité y difundida para que la conozcan todas las partes afectadas.

9.1- Datos de Carácter General Personales

La Ley Orgánica de Protección de Datos y GDD 03/2018 (LOPD) y el RGPD 679/2016, tratan de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, y resulta de aplicación a los datos de carácter personal registrados tanto informáticamente como en soporte papel.

Todos los sistemas de información de COLORIURIS se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal.

Para garantizar dicha protección, se han adoptado las medidas de seguridad que se correspondan con las exigencias previstas en la legislación de aplicación.

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con COLORIURIS.

Para más información sobre el documento de Seguridad de COLORIURIS sobre Reglamento de Protección de Datos Personales acudir a la carpeta:

- RGPD ▫ CI SG1 18.1.1 Protección de Datos Personales

9.2- 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 repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada en el informe de Análisis.

Para más información sobre la Gestión de Riesgos en COLORIURIS acudir a la carpeta:

- RIESGOS

9.3- Desarrollo de la política de Seguridad de la Información

9.3.1 – Política de Uso Aceptable

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios.

No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de los equipos están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.

- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso intencionadamente. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus.

9.3.2 – Política de puesto de trabajo despejado y escritorio limpio.

Para reducir los riesgos de accesos no autorizados, pérdida o daño de la información, tanto durante las horas de trabajo como fuera de ellas.

El personal que opere dentro de las instalaciones de COLORIURIS o con acceso a sus recursos de información, deberán siempre tener en cuenta que:

a) La información del negocio sensible o crítica, tanto en papel como en soportes de almacenamiento electrónico, debe de estar siempre guardada en armarios o muebles de seguridad, cuando ésta no sea necesaria para el usuario. La mesa de trabajo debe de quedar despejada al finalizar la jornada laboral, sin dejar al alcance de terceros ningún tipo de documentación.

b) Los ordenadores y terminales deberán quedarse apagados o protegidos mediante un mecanismo de bloqueo de pantalla y teclado controlado mediante una contraseña, así como protegidos cuando no están en uso. La responsabilidad de esto es del usuario al que se le ha asignado el equipo.

c) Deben de controlarse los puntos de entrada y salida del correo.

d) No se debe de permitir, salvo autorización expresa por parte de un responsable de la organización, el uso por usuarios no autorizados de las impresoras, escáneres y cámaras de los dispositivos móviles en la organización.

e) Los documentos que contienen información sensible o información clasificada deben de retirarse de manera inmediata de las impresoras.

9.3.3 - Seguridad de la gestión de recursos humanos

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información confidencial. El documento *CI SG1 7.3 Funciones y Obligaciones del personal*, está alojado en la carpeta EQUIPO.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede.

Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos, todo esto queda documentado.

9.3.4 - Seguridad física y del entorno

Para que una seguridad lógica sea efectiva, es primordial que las instalaciones mantengan una correcta seguridad física para evitar los accesos no autorizados así como cualquier otro tipo de daño o interferencia externa.

- Activos ▫ **CI SGI A 9**_Procedimiento CPD

9.3.5 – Dispositivos móviles

Cuando se utilicen ordenadores y dispositivos de comunicación portátiles, por ejemplo agendas, ordenadores de mano, portátiles, tarjetas inteligentes, y teléfonos móviles, se debe tener un cuidado especial para asegurar que no se compromete la información del negocio de COLORIURIS. El usuario de estos dispositivos debe de tener en cuenta los riesgos que conlleva el trabajar con el equipo móvil en entornos desprotegidos.

Todos los ordenadores portátiles de COLORIURIS deberán:

- Transportarse con los elementos necesarios para su protección física.
- Control de acceso con contraseña, que sólo deberán conocer los usuarios autorizados.
- Como regla general no deberán transportar o contener información sensible de otros proyectos que el que ha originado su salida fuera de las instalaciones de COLORIURIS.
- No deberán contener permanentemente información y ficheros del negocio, ésta debe de ser tratada en cuanto los dispositivos regresen a las instalaciones de COLORIURIS.
- Deberán tener instalados los mismos requisitos de seguridad contra los virus informáticos que el resto de equipos de COLORIURIS. Hay que asegurarse cuando se inicia el uso del dispositivo que éstos programas se hayan debidamente actualizados.
- Deberán tener instaladas las actualizaciones del fabricante del sistema operativo que hayan sido autorizadas por el departamento de sistemas.
- Se considerará la activación de sistemas de cifrado en los discos duros de los portátiles para evitar la recuperación de datos de los mismos, en caso de que éstos se extravíen, siempre que contengan información de la empresa.

En el caso de conectarse a redes públicas o externas a la de COLORIURIS deberá tenerse en cuenta:

- Como regla general, los ordenadores portátiles fuera de las instalaciones de COLORIURIS, se conectarán a través de las redes de telefonía contratadas por la empresa.
- **No está permitida** la conexión, con estos dispositivos móviles de COLORIURIS, a redes abiertas.

- No se puede conectar a redes de proveedores y/o clientes.

- En el caso de uso en zonas públicas, como salas de reuniones en oficinas de proveedor o cliente, asientos en el trasporte público o en la vía pública, fuera de las instalaciones de COLORIURIS, se tendrá especial cuidado con el uso de estos dispositivos móviles y tener cuidado para evitar el riesgo de miradas o escuchas de la conversación por personas no autorizadas.

Se debe de mantener la vigilancia continua de estos dispositivos para evitar su pérdida, robo o apropiación por personas no autorizadas.

- En caso de dejar el equipo encendido en las instalaciones del cliente por una ausencia o pausa en el trabajo, deberá bloquearse inmediatamente para evitar su uso por personas ajenas a COLORIURIS.

- En caso de extravío, hurto o robo, deberá avisarse a la Responsable de Seguridad, para que éste anule todos los contratos de comunicación vinculados, y avise a Dirección, con el fin de minimizar el impacto de la posible pérdida de información.

El personal que utiliza ordenadores portátiles y teléfonos móviles es consciente respecto a los riesgos adicionales de esta forma de trabajo y de la necesidad de aplicar permanentemente esta política.

9.3.6 - Áreas seguras

COLORIURIS toma las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.

La totalidad de las instalaciones de COLORIURIS cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen; en concreto un control de recepción e identificación del visitante y el acompañamiento del personal durante la estancia en las instalaciones.

- Registros/Evidencias ▫ **CI SG1 A 11.1.2 Control físico de entrada** (Control de accesos)

Además de tener un control de accesos donde se registra a todas las personas que acceden a las instalaciones y se le acompaña en todo momento, COLORIURIS cuenta con una puerta de entrada al edificio con llave de seguridad (llave que no se puede hacer copias), telefonillo automático y un empleado de la comunidad (Portero).
Una vez dentro del edificio, las instalaciones cuentan con dos llaves diferentes para poder acceder.

Se firmará un ACTA de entrega de llaves únicamente a los empleados de COLORIURIS autorizados, documento que está en la carpeta ACTIVOS ▫ CI SG1 A 18.1.4 Entrega de activos nadie que no este autorizado podrá acceder a las instalaciones de COLORIURIS sin previo aviso.

9.3.7 - Seguridad de los equipos

Los equipos informáticos son un activo importante del que depende la continuidad de las actividades, por lo que serán protegidos de manera adecuada y eficaz.

Los equipos informáticos de COLORIURIS están protegidos contra posibles fallos de energía (ordenador portátil con batería, SAIs, etc.).

Los equipos se mantienen de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello existe un proceso de actuación frente al posible deterioro de soportes de COLORIURIS. Sólo el **Responsable de Sistemas** como persona autorizada, podrá acceder al equipo para proceder a su reparación.

- PROCESOS ▫ **CI SG1 A 11.1.4 Procedimiento deterioro de soportes**

También se adoptan las medidas de precaución necesarias en caso de que los equipos deban abandonar las instalaciones para su mantenimiento. Se procederá a tramitar la ficha de salida de dicho soporte.

- ACTIVOS ▫ **CI SG1 A 8.3 Ficha Salida de Soportes**

9.3.8 - Equipo de usuario desatendido

Los equipos deben bloquearse, si no se están utilizando, además se configuran para que se bloquee tras 5 minutos de inactividad, procurando apagar el equipo ante una ausencia prolongada.

9.3.9 - Adquisición de productos

COLORIURIS establece un proceso formal para la adquisición de nuevos componentes del sistema:

a) Atendiendo a las conclusiones del análisis de riesgos: [op.pl.1].

b) Siendo acordes a la arquitectura de seguridad: [op.pl.2].

c) Contemplarán las necesidades técnicas, de formación y de financiación de forma conjunta para:

- La implantación inicial.
- El mantenimiento a lo largo de la vida útil.

➢ ACTIVOS ▫ **CI SG1 A 8.1.2 Recepción de nuevos activos - ACTAS**

9.3.10 - Seguridad por defecto

Se aplicará la regla de «seguridad por defecto»:

1. Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
2. Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.
3. El uso natural. Aunque el usuario no consulte el manual, será un uso seguro (siempre es seguro).

9.3.11 - Integración y actualización del sistema

En las funciones de mantenimiento, se dispone de procedimientos para analizar, priorizar y determinar cuándo y cómo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.

Todo esto aparece en la documentación de Control del cambios (CI SG1 14.2.2).

En la actualización del sistema, se mantendrá un control continuo de cambios realizados en el sistema, de forma que:

(a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no.

(b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

(c) El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.

(d) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.

(e) Mediante el análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación

- VULNERABILIDADES ▫ **CI SG1 A 12.6 Procedimiento de vulnerabilidades**

9.3.12 - Protección de la información almacenada y en tránsito

El Responsable de Sistemas garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro.

Para ello:

a) Se dispone de un registro de salida que identifique al transportista que recibe el soporte para su traslado.

b) Se dispone de un registro de entrada que identifique al transportista que lo entrega.

c) Se dispone de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.

d) Se utilizan los medios de protección criptográfica (mp.si.2 criptografía) correspondientes al nivel de calificación de la información contenida de mayor nivel.

e) Se gestiona las claves según op.exp.11 protección de claves criptográficas.

9.3.13 - Prevención ante otros sistemas de información interconectados

Dos o más sistemas de información pueden comunicarse entre sí para intercambiar información o servicios.

Se produce una interconexión de sistemas cuando:

- Existe una conexión.
- Se habilitan flujos de comunicación entre los sistemas conectados.
- Esa conexión se produce entre sistemas con diferente Responsable de Seguridad o de diferente categoría (de acuerdo con el anexo I del ENS).

Cuando en COLORIURIS se produzcan interconexiones de sistemas se atendrá:

- Al mínimo privilegio: para los usuarios y los procesos autorizados.
- Nodo auto protegido: cuando un nodo se conecta a otro, debe partir de la base de que el otro nodo no es fiable.
- Despliegue mínimo: En otras palabras, en el perímetro no habrá nada que no sea imprescindible. El objeto último es reducir la superficie de exposición a un ataque.

9.3.14 - Registro de actividad

COLORIURIS protege los registros del sistema, de forma que:

a) Se determina el periodo de retención de los registros.

b) Se asegurará la fecha y hora. Ver [mp.info.5].

c) Los registros no podrán ser modificados ni eliminados por personal no autorizado.

d) Las copias de seguridad, se ajustarán a los mismos requisitos.

e) Existe un procedimiento para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad.

f) los registros están contemplados en los procesos de copias de seguridad garantizando las seguridades mencionadas.

9.3.15 - Procedimientos operativos y responsabilidades

COLORIURIS controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello establece las interfaces adecuadas

entre la red de COLORIURIS y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red existen mecanismos para limitar los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los empleados autorizados para el manejo de información automatizada deberán estar registrados como usuarios del dominio. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario autorizado, que será único e intransferible, y su contraseña personal (CI SG1 9.4.3 Asignación de contraseñas). Esta contraseña caducará periódicamente.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación están debidamente documentados y se implementarán de acuerdo a lo que aparece en la carpeta PROCESOS ▫ Procedimientos operativos TSA. Estos procedimientos son revisados y convenientemente modificados cuando hay cambios significativos en los equipos o el software que así lo requieran.
En algunos casos será necesario que distintas áreas estén lógicamente separadas del resto para evitar accesos no autorizados.

9.3.16 - Protección frente a código malicioso y código móvil

Queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de COLORIURIS.
Todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.
Cualquier software que requiera ser instalado para trabajar sobre la red deberá ser evaluado por el Responsable de Seguridad y autorizado por el comité.
El Administrador del Sistema instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

9.3.17 - Copias de Seguridad

Los datos son guardados mediante el proceso de copias de seguridad con los que se rige en COLORIURIS.

Definido en la carpeta PROCESOS en CI SG1 A 12.3 Protocolo copias de seguridad.

9.3.18 - Gestión de la seguridad de la red

Los elementos de red (switch, router...etc.) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema.

Existirá una gestión gráfica de la red de forma que su mantenimiento pueda resultar más cómodo.

9.3.19 - Gestión de soportes

Los usuarios aplicarán las mismas medidas de seguridad a los soportes que contengan información sensible que a las existentes en las aplicaciones de donde sido extraídas.

9.3.20 - Intercambio de la Información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, etc.).

- POLÍTICAS ▫ CI SG1 7.4 Política de comunicación

9.3.21 - Seguimiento

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, etc.).

- POLÍTICAS ▫ CI SG1 7.4 Política de comunicación

9.3.22 - Controles de seguridad

Se establecen los mecanismos necesarios para permitir detectar actividades de proceso de información no autorizadas. Esto implica realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política

establecida y los procedimientos operativos así como para recomendar cualquier cambio que se estime necesario. Todas las incidencias son registradas y almacenadas en la carpeta INCIDENCIAS en el documento CI SG1 A 16 Registro de incidencias.

- Requisitos del servicio para el control de accesos

El control de acceso es protegido mediante usuario y contraseña, en base a los perfiles de las personas siendo sus privilegios los mínimos necesarios para el desarrollo de sus tareas.
CI SG1 A 6.1.2 Adecuación y Segregación de funciones

- Gestión de acceso de los usuarios

El Responsable de Sistema se encarga de proporcionar a los trabajadores el acceso a los recursos informáticos, así como el acceso lógico especializado de los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.
Cada trabajador está asociado a un perfil, de acuerdo a las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispone de unos determinados permisos y verá restringido su acceso a información y sistemas que no le son necesarios para las competencias de su trabajo.

- Responsabilidad del trabajador

Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado así como otros posibles daños. Éstos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.

- Control de acceso a la red

No se permite el acceso a la red, a los sistemas, aplicaciones o información a ningún empleado que no esté formalmente autorizado para ello.
En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con COLORIURIS para mantener el mismo nivel de seguridad que si fueran empleados de la propia organización.

Por motivos de seguridad, el acceso a la red WIFI está restringida para uso interno.

- Informática móvil y teletrabajo

Cuando los equipos o la información propiedad de COLORIURIS están fuera de las instalaciones, es el empleado que los está utilizando el que debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento, como se describe en el apartado 9.3.5. Dispositivos móviles de esta política.

- Gestión de incidencias

Cualquier empleado que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Responsable de Sistemas y de Seguridad, para que tome las medidas oportunas y registre la incidencia.

Se establecen responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad. El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.
La comunicación de incidencias se lleva mediante la plataforma de CanalDenuncias de COLORIURIS.

9.3.23 - *Continuidad del servicio*

Es imprescindible para COLORIURIS establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad de la actividad en estos casos, COLORIURIS establece planes de contingencia que permiten la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del servicio incluye, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limita las consecuencias dañinas de los mismos y asegura la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del servicio está documentado, partiendo de los riesgos detectados y de los controles definidos en consecuencia que son probados y se actualizan regularmente para comprobar su idoneidad.

La gestión de la continuidad del servicio se incorpora a los procesos de COLORIURIS y es responsabilidad de una o varias personas dentro de la entidad.

- COLORIURIS ▫ CI SG1 5.2 Plan de contingencias y continuidad de negocio

9.3.24 - *Mejora continua del proceso de seguridad*

COLORIURIS realiza una evaluación constante (objetivos e indicadores) y análisis de la respuesta a los incidentes, etc. de forma que se aprende de la experiencia, se corrigen defectos o debilidades y se busca la excelencia en la gestión del ENS. A fin de alcanzar una mejora continua.

- Registros/Evidencias ▫ CI SG1 9.1_Resultado de las métricas del SGSI
- Registros/Evidencias▫ CI SGI TABLA Registro indicadores
- Formación y mejora continua ▫ CI SGI 10.2_Plan de mejora continua
- COLORIURIS ▫ CI SG1 6.2_Objetivos SGSI
- ...

11. OBLIGACIONES DEL PERSONAL

Todos los miembros de COLORIURIS tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de COLORIURIS recibirán concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de COLORIURIS, 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.

11.1 - Terceras partes

Cuando COLORIURIS presta servicios a otros organismos o maneje información de otros organismos, se les hace partícipe de esta Política de Seguridad de la Información, se establecen canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecen procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando COLORIURIS utiliza servicios de terceros o ceda información a terceros, se les hace partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte queda sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecen procedimientos específicos de reporte y resolución de incidencias. Se garantiza que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requiere un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.