INDICE

1. Introducción
2. Objetivos
3. Marco Regulatorio
4. Roles de seguridad
5. Comité de Seguridad. Estructura
6. Directrices para la estructuración de la documentación de seguridad del sistema.
   - 6.1. POLITICA DE GESTION DE ACTIVOS
   - 6.2. POLITICA DE GESTION DE PERSONAS
   - 6.3. POLITICA DE SEGURIDAD FISICA Y AMBIENTAL
   - 6.4. POLITICA DE COMUNICACIÓN Y OPERACIONES
   - 6.5. POLITICA DE CONTROL DE ACCESOS
   - 6.6. POLITICA DE CONTROL Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION
   - 6.7. POLÍTICA DE GESTIÓN Y CONTROL DE INCIDENTES
   - 6.8. POLITICA DE CONTINUIDAD DEL SERVICIO
   - 6.9. POLITICA DE CUMPLIMIENTO DE LA NORMATIVA LEGAL
   - 6.10. POLITICA DE ACUERDOS DE NIVEL DE SERVICIO
   - 6.11. POLITICA DE RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACION
   - 6.12. POLITICA DE USO DE LA RED
   - 6.13. POLITICA DE SEGURIDAD CRIPTOGRAFICA
   - 6.14. POLITICA DE MEJORA CONTINUA
   - 6.15. POLITICA DE CONTROL DEL RIESGO
   - 6.16. POLITICA DE ACEPTACION Y PUESTA EN SERVICIO DE SOFTWARE
   - 6.17. POLITICA DE PROTECCION FRENTE A CODIGO DAÑINO
   - 6.18. POLITICA DE EQUIPO DESANTENDIDO
   - 6.19. POLITICA DE ESCRITORIO Y PANTALLA LIMPIA
7. Riesgos derivados del tratamiento de los datos personales.

1.- INTRODUCCIÓN

La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. **Este documento es aprobado por la Alta Dirección de la corporación**. A tal efecto, este instrumento incluirá los siguientes puntos a desarrollar:

- Los objetivos o misión de la organización.
- El marco regulatorio en el que se desarrollarán las actividades.
- Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.
- La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
- Los riesgos que se derivan del tratamiento de los datos personales.

Las organizaciones tenemos que disponer de mecanismos para el control y gestión de la seguridad de la información (Internet, la nube, Big Data, Internet de las cosas (IoT), IA, etc.) que manejamos. Este hecho tiene una gran trascendencia tanto para las empresas como para la sociedad, derivado del cambio de paradigma:

- El mundo físico y digital están hiperconectados.
- Los usuarios son un elemento activo.
- La información es procesada, almacenada y transmitida sin restricciones.

LLOOL es una empresa especializada en la provisión de servicios para el mantenimiento, soporte y supervisión de la infraestructura y seguridad informática de empresas de cualquier sector, cuya misión busca obtener una mejora en el rendimiento de la infraestructura, mejorar la productividad del personal técnico y reducir significativamente el coste de las inversiones.

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen

o administren los sistemas de información y comunicaciones. También estará a disposición de otros grupos de interés externos, una versión abreviada que se publicará en la web corporativa https://www.llooltec.com junto con las políticas de privacidad.

La eficacia y aplicación del Sistema de Gestión de la Seguridad de la Información es responsabilidad directa del Comité de Seguridad que estará formado principalmente por la Dirección, que es responsable de la aprobación, difusión y cumplimiento de la presente Política de Seguridad. En su nombre y representación se ha nombrado un Responsable de Seguridad de la Información, que posee la suficiente autoridad para desempeñar un papel activo en el Sistema de Gestión de la Seguridad de la Información, supervisando su implantación, desarrollo y mantenimiento.

Los diferentes roles junto con sus respectivas funciones y responsabilidades están reflejados en el **manual de funciones (MG02)** que forma parte de la documentación del sistema de gestión de la información. En especial las categorías de seguridad de los sistemas de información será determinar los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS; así como de la implantación y actualización del Sistema de gestión de la seguridad de la información y ENS, asumiendo las responsabilidades de planificación y mejora organizativa. Este será designado por el Comité de Seguridad de la información y renovará su cargo cada cuatro años.

Esta política de seguridad será revisada con una periodicidad anual o cuando se produzcan cambios significativos que la afecten con el fin de mantener la idoneidad, adecuación y eficacia.

2.- OBJETIVOS:

El objetivo de esta Política de Seguridad es fijar el marco de actuación necesario para proteger los recursos de información frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad de la información.

La política de seguridad se desarrollará aplicando los siguientes requisitos:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

En LLOOL, toda persona cuya actividad pueda, directa o indirectamente, verse afectada por los requisitos del Sistema de Gestión de la Seguridad de la Información, está obligada al cumplimiento estricto de la Política de Seguridad de la Información, implantando las medidas necesarias para cumplir la normativa aplicable en materia de seguridad en general y de seguridad informática, relativa a la política informática, a la seguridad de edificios e instalaciones y al comportamiento de empleados y terceras personas asociadas a la Organización en el uso de sistemas informáticos.

3.- MARCO REGULATORIO

Las medidas necesarias para garantizar la seguridad de la información mediante la aplicación de normas, procedimientos y controles nos permiten llevar a cabo los siguientes compromisos:

Cumplir con los requisitos aplicables en materia de los sistemas de información. Se tendrá en cuenta de forma especial:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos

Personales y garantía de los derechos digitales.

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (reglamento General de Protección de Datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- El convenio colectivo aplicable, correspondiente a “Consultoría de estudio de mercado y de servicios informáticos”.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- RD-ley 13/2012 de 30 de marzo, ley de cookies.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Los requisitos legales que aplican a esta organización en el desarrollo de la Política de Seguridad se actualizan en el documento **PG14-F1 Listado de Requisitos Legales**.

4. ROLES O FUNCIONES DE SEGURIDAD, DEFINIENDO PARA CADA UNO, SUS DEBERES Y RESPONSABILIDADES, ASÍ COMO EL PROCEDIMIENTO PARA SU DESIGNACIÓN Y RENOVACIÓN.

Los roles y funciones de seguridad su definición y la renovación de responsabilidades se definen en el procedimiento **PG02.ANEXO I Categorización del sistema**.

5.- COMITÉ DE SEGURIDAD. ESTRUCTURA

El comité de seguridad estará formado por los siguientes responsables:

- Responsable de Seguridad
- Responsable de Servicio
- Responsable Técnico

El comité tendrá una vigencia de cuatro años.

Las funciones que tendrá el Comité de Seguridad son las siguientes:

Se dispone un comité de seguridad, que deberá asumir la tarea general del desarrollo y la implementación de la seguridad y fundamente la identificación de medidas de seguridad. Dentro de la tarea general del desarrollo y la implementación de la seguridad se pueden destacar estas áreas que son competencia directa del Comité de Seguridad:

- Elaboración y mantenimiento de la política de seguridad.
- Gestión de acuerdos de nivel de servicio (SLA).
- Evaluar los Riesgos y amenazas sobre los Activos.
- Definición de responsabilidades y segregación de funciones.
- Clasificación de la información.
- Gestión de auditorías de seguridad.
- Implementación del Sistema de Gestión de la Seguridad.
- Implementar ENS
- Implementar ISO: 27001 Seguridad
- Implementar ISO: 22301 Continuidad de negocio

El Comité de Seguridad elaborará un informe anual de la aplicación de las políticas de seguridad de la organización. El informe de **Revisión del Sistema** debe de incluir la siguiente información:

- Estado de las acciones de revisiones por el comité del ejercicio anterior.
- Cambios en el sistema de Gestión De La Organización.
- Revisión de las Políticas de Seguridad.
- Informe sobre el comportamiento de las políticas de seguridad.
- Resultado de auditorías, Observaciones, No Conformidades y acciones correctivas.
- Seguimiento y resultados de los indicadores.
- Grado de cumplimiento de los objetivos de gestión.
- Plan de tratamiento de riesgos y amenazas.
- Resultado del análisis de riesgos.
- Mejoras en el sistema de gestión.
- Formación y capacitación.
- Recursos humanos.

- Acciones relacionadas con los recursos.
- Informe de Proveedores.
- Conclusiones finales.

Las responsabilidades de los Responsables de Seguridad, Responsable de Servicio y Reponsable Técnico están definidas en el procedimiento **PG02. ANEXO I CATEGORIZACIÓN DEL SISTEMA** y en la matriz **PG99 AUTORIZACIONES**.

6.- DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA

6.1.- POLITICA DE GESTION DE ACTIVOS

En LLOOL se realiza una protección adecuada de los activos (incluyendo mantenimiento, inventario y clasificación), identificando a los propietarios de estos activos, cuya responsabilidad es el mantenimiento de los controles adecuados sobre los mismos. A tener en cuenta todos los medios o soportes que transmiten, almacenan y procesan información. Por ejemplo: los ordenadores portátiles, las comunicaciones móviles, etc.

También se realiza una clasificación de los mismos ya que hay que asegurar que la información recibe un nivel de protección apropiado. Este aspecto tiene especial incidencia sobre la garantía de confidencialidad, aun así, es importante reseñar que la asignación de responsables por activo y el deber de éstos últimos de cumplir con las políticas de seguridad sobre estos activos hace que sea un dominio horizontal a las garantías de seguridad definidas en la introducción: confidencialidad, integridad, disponibilidad, autenticidad y conservación de la información.

Se mantiene un inventario de los activos de información de las aplicaciones informáticas que sirven de soporte a la tramitación telemática, velando porque exista un responsable o propietario para cada uno de los mismos. Este inventario se actualiza de forma regular.

6.2- POLITICA DE GESTION DE PERSONAS

En LLOOL se garantizará que cualquier persona que tenga acceso a los activos inventariados dentro del ámbito de aplicación de esta política (incluidas personas que trabajan nuestro nombre) sepan y acepten sus responsabilidades en materia de

seguridad de los sistemas de información y recursos con los cuales trabajan durante todo el ciclo de vida del empleado (antes de la contratación, durante la contratación y una vez finalizado la relación laboral). La principal garantía que se quiere cubrir es la confidencialidad mediante el uso de cláusulas referentes a obligaciones y responsabilidades del empleado y contratistas. También se pretende reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

Desde LLOOL se proporcionará la formación y concienciación adecuada a los usuarios en lo que respecta a la presente política de Seguridad de la información, incluyendo requerimientos de seguridad y responsabilidades legales. La seguridad eficaz depende, en parte, de que los usuarios sepan lo que se espera de ellos y cuáles son sus responsabilidades, comprometiéndose con las mismas. Éstos deben conocer los motivos de las medidas de seguridad física y lógica establecidas y también las consecuencias de violar la seguridad.

Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo electrónico de alguien más (mientras esta persona se encuentra fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la Organización.

Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de LLOOL. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

6.3.- POLITICA DE SEGURIDAD FISICA Y AMBIENTAL

La infraestructura, así como los soportes de almacenamiento de información que residan en nuestros edificios y en los proveedores de servicio o terceros, estarán protegidos contra daño físico o hurto, utilizando mecanismos de control de acceso físico, que aseguren que únicamente el personal autorizado tiene acceso a los mismos.

Con esta finalidad, dicha infraestructura estará ubicada en áreas de acceso restringido, con diferentes niveles de seguridad, a las cuales únicamente pueda acceder personal debidamente autorizado. Los accesos a cada uno de los niveles deben ser registrados por mecanismos de control de acceso, quedando disponibles para su control en auditorías.

Los sistemas y la información que soportan, estarán adecuadamente protegidos frente a amenazas físicas o ambientales, sean éstas intencionadas o accidentales.

6.4.- POLITICA DE COMUNICACIÓN Y OPERACIONES

Se establecerán responsabilidades y se definirán procedimientos para la gestión y operación de todos los medios de tratamiento de información. Esto incluye elaborar de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.

Se implantará la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso de la infraestructura deliberado o por negligencia.

Se requieren ciertas precauciones para prevenir y detectar la introducción de software dañino. El software y los recursos de tratamiento de información son vulnerables a la introducción de software dañino como virus informáticos, gusanos de la red, caballos de Troya y bombas lógicas.

Los usuarios deben conocer los peligros que tiene el software dañino o no autorizado; y se implementarán controles y medidas especiales para detectar o evitar su introducción en puestos de trabajo, servidores y pasarelas de conexión a redes públicas o privadas necesarias para evitar la infección de los sistemas de información por virus o cualquier otro tipo de software dañino. En particular es esencial que se tomen precauciones para detectar o evitar los virus informáticos en los ordenadores personales. Es de obligado cumplimiento la actualización periódica y regular de los mecanismos antivirus.

Se establecerán procedimientos rutinarios para conseguir la estrategia aceptada de respaldo haciendo copias de respaldo, ensayando su oportuna restauración, registrando eventos o fallos y monitorizando el entorno de los equipos cuando proceda.

La gestión de la seguridad de las redes que cruzan las fronteras de nuestra Organización requiere una atención que se concreta en controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas. Se deben establecer los controles necesarios que impidan la suplantación del emisor, modificación o pérdida de la información transmitida, tanto en las comunicaciones con sistemas situados en las redes internas, como con aquellos sistemas externos, independientemente de la plataforma, protocolos o aplicaciones que las soporten.

Se establecerán los procedimientos adecuados para proteger los documentos, soportes informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema frente a daño, robo y acceso no autorizado. El almacenamiento, manipulación, transporte, la destrucción o desecho de cualquier activo de información, que contenga información sensible deberá garantizar la imposibilidad de acceso o recuperación de su contenido por parte de personal no autorizado.

Se controlarán los intercambios de información y software entre organizaciones, que deben cumplir con toda la legislación vigente. Se realizarán los intercambios sobre la base de acuerdos formales. Se establecerán procedimientos y normas para proteger los soportes en tránsito.

Por otra parte, para detectar y evitar posibles brechas o problemas que pudieran estar presentes en la organización a nivel de seguridad relativa al entorno técnico, el sistema de gestión de la seguridad se debe revisar regularmente. Estas revisiones deben realizarse en base a las medidas de seguridad que apliquen a la información y deben ser auditados en cumplimiento con los estándares de implementación de seguridad aplicables y los controles de seguridad documentados.

Los responsables (de los activos de la información) deben revisar regularmente el cumplimiento del procesamiento de la información dentro de su área de responsabilidad con las políticas y medidas de seguridad apropiadas, y cualquier otro requerimiento de seguridad.

Si se encuentra cualquier incumplimiento como resultado de la revisión, los responsables deben actuar para determinar cuál es la causa y establecer una acción correctiva. Las revisiones y acciones deben quedar registradas.

El chequeo del cumplimiento técnico debe ser realizado por una persona con competencia (p.e. ingeniero de sistemas) y autorizado explícitamente para realizar dicha labor.

6.5.- POLITICA DE CONTROL DE ACCESOS

Los permisos de acceso a las redes, sistemas y a la información que esos soportan se otorgarán de modo que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

Se establecerán procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios. Estos procedimientos cubrirán todas las etapas del ciclo de vida del acceso a usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios. Se prestará especial atención si cabe al necesario control de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios evitar los controles del sistema.

Todos los accesos realizados a las bases de datos, llevarán asociado un proceso de identificación, autenticación y autorización. Se establecerán mecanismos de registro, monitorización de acceso y uso de los sistemas.

Las credenciales de acceso de cada usuario serán personales e intransferibles. Toda persona registrada que disponga de credenciales de acceso será responsable de mantener su confidencialidad y asegurar su correcto uso. Se establecerán los mecanismos necesarios en los sistemas para impedir la visualización de las credenciales por parte de terceras personas.

Debido a que una protección efectiva necesita la cooperación de los usuarios autorizados, los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de la efectividad de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

El acceso a los servicios desde redes externas e internas debe ser controlado de forma tal que se asegure que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por medio de:

- Interfaces adecuadas entre la red de LLOOL y las redes públicas o las privadas de clientes o administraciones.
- Mecanismos adecuados de autenticación para los usuarios y los equipos.
- Control de los accesos de los usuarios a los servicios de información.

El acceso remoto desde redes públicas debe garantizar la confidencialidad de la información que se transmite, así como la identidad de los usuarios autorizados a hacer uso del servicio de acceso remoto mediante mecanismos de autenticación fuerte. Se necesita restringir el acceso a los ordenadores para permitir sólo usuarios autorizados. Los ordenadores que atienden a múltiples usuarios deberían ser capaces de:

- Identificar y verificar la identidad de cada usuario autorizado (y si procede, el terminal o la ubicación física del mismo).
- Suministrar mecanismos de gestión de contraseñas que garanticen la calidad de las mismas.
- Cuando proceda, restringir la conexión de usuarios o ventanas horarias.

Con la finalidad de detectar y reaccionar ante comportamientos sospechosos o inesperados, se establece y activan sistemas de registro de actividades que almacenan los datos generados por las actividades de sistemas, aplicaciones y usuarios en los activos de información.

Se establecerán normativas, procedimientos y medidas técnicas específicas para la protección de sistemas portátiles, dispositivos móviles y accesos remotos de teletrabajo.

El usuario que tenga bajo su resguardo algún equipo portátil, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo. Los equipos personales, tienen el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

En caso de desaparición, robo o extravío del equipo portátil o accesorios que dispongan de información y que estén bajo resguardo de un usuario, deberá dar aviso de inmediato al responsable técnico, para iniciar el registro y control de incidencias e interponer la denuncia ante la autoridad competente, si fuera necesario.

6.6.- POLITICA DE CONTROL Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION

El control y mantenimiento de las aplicaciones dentro del ámbito especificado debe incluir los controles y registros apropiados que garanticen la correcta implementación de las especificaciones de seguridad y se llevará a cabo teniendo en cuenta las mejores prácticas de seguridad en la programación. Especialmente, se usarán sistemas y técnicas criptográficas –cifrado, firma digital, no-repudio–para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

La información incluida en los soportes, debe estar protegida contra modificaciones no autorizadas empleando mecanismos que aseguren la integridad de la misma. Se dispone de las guías, estándares, recomendaciones y procedimientos necesarios para facilitar la inclusión de la seguridad durante las etapas del ciclo de vida de desarrollo, tales como uso de controles criptográficos, gestión de claves, programación segura, etc.

Los entornos que forman parte del ciclo de vida de desarrollo informático estarán convenientemente separados o segmentados en todos y cada uno de los sistemas. Asimismo, y con la finalidad de evitar el acceso o divulgación de datos que residan en los entornos, se debe controlar el intercambio de datos reales entre el entorno de producción y el resto de entornos.

En los entornos de pruebas o desarrollo, para las aplicaciones, o infraestructura deben estar disponibles juegos de datos de prueba, preparados específicamente, donde las relaciones entre datos y personas hayan sido disociadas o enmascaradas. En cualquier caso, antes de utilizar un nuevo sistema de gestión de información o software no comercial, se debe de validar previamente.

6.7.- POLÍTICA DE GESTIÓN Y CONTROL DE INCIDENTES

Se exigirá a todos las personas, que se informen con la mayor celeridad posible (ante cualquier debilidad observada o sospecha). Para ello se establecerán los procedimientos y cauces adecuados sobre concienciación, formación y capacitación en seguridad de la información.

Así mismo, se debe garantizar que se aplica una metodología sólida para la gestión de incidentes de seguridad (establecer responsabilidades y procedimientos), a la vez que emplear procesos de mejora continua y métodos para la recogida de evidencias.

Se dispondrá de un mecanismo que permite la monitorización de las incidencias de seguridad, cuantificación y costes asociados de las mismas, así como la recopilación de evidencias.

Se establecerán procedimientos formales para informar y priorizar eventos de seguridad. Todo el personal afectado deberá conocer los procedimientos para informar de los diferentes tipos de eventos y debilidades que pudieran impactar en la seguridad de información.

Se establecerán responsabilidades y procedimientos formales para manejar los eventos de seguridad y debilidades con eficacia una vez que éstas hayan sido comunicadas. Además, se establecerá un proceso formal de mejora continua sobre toda la gestión de incidentes de seguridad.

Se recopilarán las evidencias necesarias por cada incidente con el fin de cumplir con la legalidad vigente y la mejora continua del Sistema de seguridad de la información.

El procedimiento de reporte de incidencias deberá incluir:

- Procesos de notificación adecuados para asegurar que aquellos que reportan eventos en la seguridad de la información sean notificados de los resultados después de haber tratado y terminado con el problema.
- Formatos de reporte los eventos en la seguridad de la información para respaldar la acción de reporte, y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento en la seguridad de la información.
- Indicaciones para actuar de forma correcta en caso de ocurrencia de un evento de seguridad:
    - Anotar todos los detalles importantes inmediatamente (por ejemplo, el tipo de no cumplimiento o violación, mal funcionamiento actual, mensajes en la pantalla, conducta extraña);
    - No llevar a cabo ninguna acción por cuenta propia, sino reportar inmediatamente al punto de contacto;
    - Referencia a un proceso disciplinario formal establecido para tratar con los usuarios empleados, o externos que cometen violaciones de seguridad.

Para garantizar una gestión de incidentes efectiva, se establecerán las responsabilidades y procedimientos necesarios para manejar de manera adecuada los eventos y debilidades en la seguridad de la información una vez que han sido reportados.

Se aplicará un proceso de mejora continuo para la respuesta, monitorización, evaluación y la gestión general de los incidentes en la seguridad de la información. Cuando se requieran evidencias, estas se recogerán cumpliendo con los requerimientos legales.

Además de reportar los eventos y debilidades en la seguridad de la información, se utilizará la monitorización de los sistemas, alertas y vulnerabilidades para detectar los incidentes en la seguridad de la información. Se tendrá en cuenta:
Deben existir diferentes actuaciones para manejar los diferentes tipos de incidentes de seguridad. Estos incluirán:

- Análisis de la causa del incidente.
- Contención.
- Implementación de la acción correctiva.
- Comunicaciones a los afectados.
- Reporte de la acción a los interlocutores apropiados

.

Se acordarán con la dirección los objetivos para la gestión de incidentes de seguridad de la información y se garantizará que los responsables e implicados en la resolución de las mismas entiendan las prioridades de la organización para el manejo de los incidentes en la seguridad de la información.

6.8.- POLITICA DE CONTINUIDAD DEL SERVICIO

Se deberá implementar un proceso de gestión de continuidad de actividad para garantizar la recuperación de los procesos críticos de la organización, en caso de desastre, reduciendo el tiempo de indisponibilidad a niveles aceptables, desde el punto de vista de la actividad, mediante la adecuada combinación de controles de carácter organizativo, tecnológico y procedimental, tanto preventivos como de recuperación.

Este proceso se desarrollará mediante un Plan de Continuidad del negocio que debe ser probado de forma periódica y regular y que se debe mantener actualizado en todo momento. Para ello, se debe evaluar el riesgo y el impacto asociado ocasionado por la ausencia de continuidad de los sistemas de información que den soporte o estén implicados en la actividad de LLOOL.

Estos planes deben contemplar, como mínimo, los riesgos más probables que puedan afectar a la continuidad de los procesos de la Organización y permitir que los recursos previstos para superar la contingencia se encuentren disponibles y aseguren la continuidad de dichos procesos en el tiempo máximo establecido en cada uno de ellos.

6.9.- POLITICA DE CUMPLIMIENTO DE LA NORMATIVA LEGAL

Es responsabilidad de todas las áreas implicadas conocer y cumplir la legislación vigente de aplicación en sus ámbitos de actuación. Específicamente, se deben contemplar los mecanismos y procedimientos indicados por el marco legislativo de referencia de Protección de Datos Personales y Garantía de los Derechos Digitales, Servicios de la Sociedad de la Información y de comercio electrónico y de la Propiedad Intelectual.

El personal de LLOOL adquiere el deber de secreto, es decir, la responsabilidad de no divulgar ningún tipo de información que haya adquirido en la realización de su trabajo, tanto interna como de los clientes u otros grupos de interés.

Las aplicaciones que sirven de soporte para el control de la información, se someterán periódicamente a una auditoría, encargada de verificar el cumplimiento de la normativa de seguridad y de los procedimientos e instrucciones vigentes en materia de seguridad de la información. El proceso de auditoría debe verificar el cumplimiento de las iniciativas de seguridad planificadas a corto plazo, realizar periódicamente revisiones del grado de instauración de los controles y de su efectividad desde el punto de vista de la seguridad y ser independiente de las comprobaciones realizadas internamente por la organización.

Se establecerán las medidas necesarias para evitar la desactivación, accidental o malintencionada, de los mecanismos de seguimiento y auditoría.

6.10.- POLITICA DE ACUERDOS DE NIVEL DE SERVICIO

Es prioritario mantener la seguridad de la información que pueda ser manejada por externos. Para ello es importante gestionar la seguridad desde el momento que se formalizan los contratos con externos y proveedores. Esto es:

- Antes de acordar el acceso de externos, se debe identificar cuáles son los principales riesgos de seguridad de los activos que se van a manejar para formalizar las medidas concretas más acordes a cada casuística concreta. La adopción de dichas medidas quedará reflejada y formalizada en el contrato que se realice con el externo.
- Incluir análisis de riesgos de los activos.
- Los acuerdos o contratos con externos que involucran el acceso a los activos de la información, o agregan productos/servicios/otros a la misma deben

abarcar todos los requerimientos de seguridad que establece esta politica.

- Además, se desarrollarán Acuerdos de Nivel de Servicio (en adelante, ANS o SLA en sus siglas en inglés) con el fin de fijar y formalizar el nivel de calidad de servicio acordado.

6.11.- POLITICA DE RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACION

Todas las responsabilidades en el ámbito descrito de seguridad deben estar claramente definidas, teniendo en cuenta que:

- La asignación de las responsabilidades en el ámbito descrito de seguridad debe realizarse en concordancia con la política de seguridad definida.
- Se deben definir claramente las responsabilidades para la protección de los activos y para llevar a cabo los procesos de seguridad.
- Cuando se considere necesario, esta responsabilidad debe ser complementada con un alineamiento más detallado para áreas y medios de procesamiento de información específicos.

Los trabajos de dichas áreas se acometerán dentro de un marco de trabajo orientado a procesos. Se deberá introducir en todos los ámbitos de la seguridad donde sea posible la segregación de funciones con el fin de que nadie pueda tener acceso, modificar o utilizar los activos sin autorización o detección. Se debiera separar la iniciación de un evento de su autorización y se debiera considerar la posibilidad de colisión en el diseño de los controles.

6.12.- POLITICA DE USO DE LA RED

Se deberá prevenir el acceso no autorizado a los servicios de red sean estos internos o externos. Si bien estos accesos a servicios de acceso remoto serán autorizados si respondan a necesidades de actividad, mantenimiento y soporte. Se tomarán las siguientes medidas de control:

- Se establecerán mecanismos para tratar convenientemente la información

transmitida, los sistemas y recursos accedidos, la identidad de las personas que realizan dichos accesos y las posibles implicaciones que el acceso en global conlleva.

- Los servicios de acceso remoto deberán de disponer de mecanismos de autenticación basados, cuando menos, en el doble factor de autenticación más el binomio usuario-contraseña (siempre a través de canal cifrado) o criptografía de clave pública. Al mismo tiempo, dependiendo de la criticidad de la información, la comunicación deberá estar cifrada. De manera imprescindible, la contraseña deberá transmitirse siempre de forma ininteligible.
- Los usuarios con privilegios de acceso remoto deberán asegurar que su equipo cuando está conectado de forma remota a la red corporativa, no estará simultáneamente conectado a ninguna otra red privada.
- Es responsabilidad de los empleados con privilegios de acceso remoto asegurar que éste no es usado por empleados no autorizados o externos a LLOOL. Los empleados con posibilidad de acceder remotamente a la red interna deberán recordar constantemente que las conexiones remotas entre su equipo y la de la organización son extensiones literales de la red corporativa, y que proporcionan una vía de acceso potencial hacia información confidencial.
- Los empleados deberán tomar todas las medidas posibles y razonables para proteger los activos de LLOOL. Por ello, estará prohibido transmitir identificadores de usuario, contraseñas o credenciales, configuraciones de la red interiores o direcciones a través de Internet. En caso de necesidad esta información se enviará cifrada.
- Las conexiones que se llevan a cabo entre redes deben permitir únicamente el tráfico estrictamente necesario y autorizado. Para ello se deben utilizar elementos de filtrado (como cortafuegos) que definan el perímetro de cada red conforme a las normas de interoperabilidad establecidas.
- El criterio de separación de redes mediante perímetros persigue la segmentación en redes físicamente independientes, agrupando componentes con requisitos o características similares desde el punto de vista de seguridad de la información.
- Los flujos de tráfico entre redes situadas en distintos perímetros de seguridad se basarán en los tipos de tráfico permitidos y no permitidos entre ellas.
- Con el fin de ocultar los esquemas internos de direccionamiento IP, además de para solucionar problemas derivados de conflictos en planes de

direccionamiento se debe poder hacer uso de mecanismos de traducción de direcciones (p. ej. NAT).

6.13.- POLITICA DE SEGURIDAD CRIPTOGRAFICA

Aquellos sistemas de información que precisen gestionar claves criptográficas, deberán disponer del software necesario para gestionarlas y cifrar la información, debiendo permitir:

- Generación de claves.
- Distribución de claves empleando un canal seguro.
- Activación de claves.
- Almacenamiento y acceso a las claves. Las claves deberán estar fuertemente protegidas físicamente y sólo permitido el acceso a las mismas con las más estrictas autorizaciones con el fin de preservar su confidencialidad.
- Cambio o actualización de claves. En caso de cambio, se deberá aplicar un proceso de redistribución de la nueva clave y, en su caso, abandono y/o destrucción de la anterior.
- Compromiso de las claves. Se deberán establecer procedimientos y responsabilidades para la notificación del compromiso de las claves, así como de las medidas a tomar en aquellas situaciones que pongan en peligro la confidencialidad de las mismas.
- Recuperación de claves. En caso de pérdida o deterioro de claves criptográficas, se deberán establecer procedimientos, responsabilidades y mecanismos para la recuperación de claves especificando las condiciones necesarias para proceder a la recuperación, de forma que se garantice el acceso a la información que haya sido cifrada con dichas claves.
- Archivado de claves (fideicomiso de claves). En los casos en que los requisitos de confidencialidad sean elevados, se deberán emplear técnicas de división de claves en diferentes localizaciones o a diferentes figuras, de modo que se asegure que la custodia de las mismas se realiza sólo en condiciones de máxima seguridad.
- Destrucción de claves. Se deberán establecer procedimientos y responsabilidades para la destrucción de claves, donde se asegure que no existen datos que hayan sido cifrados usando dichas claves.
- Registro de las operaciones relacionadas con la gestión de claves. Se deberán mantener registros de las actividades realizadas, registrando, al menos:

- Los destinatarios de las claves simétricas.
- Los responsables de cada actividad.
- La fecha de realización de cada una de las actividades.

La selección de los algoritmos a utilizar deberá estar publicados en la guía CCN-STIC 221 Guía de mecanismos criptográficos autorizados en el caso de que no figuren deberán de cumplir lo expecifcaconsiderar la legislación vigente relativa al uso de mecanismos de cifrado. Otros aspectos a considerar en la selección de algoritmos de cifrado deberán ser la fortaleza y la eficiencia del algoritmo, así como el tipo de cifrado, simétrico o asimétrico.

La longitud de las claves de cifrado será acorde al periodo de tiempo durante el cual se pretende asegurar la confidencialidad de los datos que se van a cifrar.

Las claves de cifrado se considerarán información secreta y, como tal, su acceso deberá estar limitado al propietario de las mismas. Las claves de cifrado se deberán generar por medios que garanticen su fortaleza. Todo programa o archivo que contenga fórmulas, algoritmos u otras especificaciones que se utilicen para la generación de claves debe estar controlado con las máximas medidas de seguridad.

Las claves de cifrado deben ser ininteligibles y no se deben incluir dentro de los programas software. Los ordenadores y sistemas de comunicación deben tener implementados controles que impidan la recuperación de las claves almacenadas.

Cuando sea necesario asegurar la disponibilidad de la información cifrada se utilizarán sistemas de cifrado que dispongan de recuperación de claves.

Para la selección de soluciones de cifrado adecuadas a las necesidades de las aplicaciones y la información se establecerán las siguientes especificaciones de seguridad:

- Se identificará la normativa de carácter legal o regulatoria referente a controles de cifrado.
- Para cada caso se deberá determinar el algoritmo de cifrado que se empleará para preservar la confidencialidad de la información, realizando un análisis cuyo resultado especifique al menos los siguientes requerimientos de seguridad:

- Utilización del algoritmo o solución

Nivel donde se procederá al cifrado de la información:

- En transmisión, pudiendo cifrarse dentro de la aplicación o en la transmisión.
- En almacenamiento, pudiendo cifrarse la base de datos o sistema de ficheros.

Escalabilidad de la solución, considerando las necesidades de expansión futura, en particular el sistema de intercambio de claves deberá ser adecuado, teniendo en cuenta que las soluciones basadas en secreto compartido no escalan de forma adecuada.

Funcionalidades adicionales soportadas por la solución escogida, tales como:

- Soporte para diferentes métodos de intercambio de claves.
- Número de algoritmos de cifrado que soporta para intercambio con otros sistemas.

Método de cifrado soportado por la solución:

- Cifrado por hardware
- Cifrado por software

Posibilidades de ampliación futura de la solución, incorporando nuevas operaciones criptográficas.

En los sistemas de información y comunicaciones se usará la técnica de firma electrónica cuando sea necesario garantizar el no repudio del mensaje o transacción mediante la autenticidad de origen y la integridad de la información.

La utilización de la técnica de firma, en los términos establecidos por la legislación vigente, supone el uso de certificados digitales emitidos por una autoridad de certificación reconocida.

6.14.- POLITICA DE MEJORA CONTINUA

Se implementará un procedimiento para garantizar la mejora continua en el ámbito de la seguridad de la información. Para cumplir con este principio se necesita disponer de la información necesaria para responder preguntas sobre la eficiencia, eficacia, nivel de madurez o nivel de implantación del sistema de seguridad.

Para esta finalidad se pueden utilizar métricas e indicadores que permitan medir la eficacia de las medidas de seguridad para verificar el cumplimiento de los requisitos de seguridad.

Una vez conocido el estado en que se encuentra en materia de seguridad se estará en disposición de tomar las decisiones oportunas en el momento idóneo gestionando de forma proactiva (antes que se produzcan situaciones y/o escenarios no deseados) la seguridad de la información de forma eficiente.

6.15.- POLITICA DE CONTROL DEL RIESGO

La evaluación del riesgo debe incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

Las evaluaciones del riesgo deben identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados deben guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar las medidas de seguridad seleccionadas para protegerse contra las amenazas tanto internas como externas.

6.16.- POLITICA DE ACEPTACION Y PUESTA EN SERVICIO DE SOFTWARE

Para Minimizar el riesgo de corrupción de software durante el proceso de implantación en los entornos de producción se deberá considerar:

- La actualización de las librerías de programas sólo se debe realizar tras haber concluido con éxito las correspondientes pruebas y tras obtener la autorización del usuario final.
- Las actualizaciones serán realizadas por técnicos especialistas y quedarán registradas en el control de actualizaciones.
- Será necesaria una autorización por escrito del responsable del activo.

- Se mantendrá exclusivamente el código ejecutable.
- El código ejecutable no será pasado al entorno de producción hasta que no se hayan realizado pruebas y el resultado haya sido aceptado.
- Las características o funcionalidades que sean innecesarias en el entorno de producción se identificarán y desactivarán en el momento de la instalación del software.
- Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías del entorno de pruebas a las librerías del entorno de producción, sin que previamente sean compilados por el área asignada.
- Las versiones anteriores se mantendrán como medida de seguridad. Se realizarán las copias de seguridad necesarias antes del pase al entorno de producción.
- Para cada aplicación, deberán existir procedimientos de gestión de errores que permitan la trazabilidad de éstos.
- Antes de realizar modificaciones del software, deberán revisarse los contratos de mantenimiento con los externos del mismo, ya que muchos de ellos no permiten que el cliente las realice sin su autorización.
- Si existe la posibilidad, para el paso desde los entornos de desarrollo o pruebas al entorno de producción, se utilizarán herramientas automáticas que realicen un control de versiones de software y permitan restaurar los sistemas en caso de fallo.
- Como medida de precaución ante posibles desastres se debe mantener un registro de todas las actualizaciones de las librerías de programas y se deben almacenar durante un tiempo las versiones anteriores.
- Las mismas precauciones se deben aplicar al software adquirido a terceros, en este caso se deben considerar las indicaciones de soporte del proveedor.

6.17.- POLITICA DE PROTECCION FRENTE A CODIGO DAÑINO

Se debe de asegurar la protección de la integridad del software y de la información ante amenazas concretas de tipo lógico (malware en general). Para ello se tendrá en cuenta:

- Todos los componentes de la ITT deberán tener una configuración segura (securización) antes de conectarse a cualquier tipo de red.
- La securización deberá ser especialmente restrictiva en los cortafuegos, equipos para garantizar la seguridad del entorno y en aquellos sistemas ubicados en segmentos de red expuestos a Internet u otras redes públicas.
- La implantación de la configuración segura será llevada a cabo por los

responsables correspondientes.

- Las medidas de securización o parámetros de configuración segura, una vez definidas, analizadas y probadas, deberán incluirse en el plan de instalación de equipos.
- Los parámetros de configuración segura dependerán de la clasificación del activo en si mismo.
    - De la información que traten y de los grupos de usuarios que acceden. Los usuarios y grupos de usuarios que acceden al sistema, así como la clasificación de la información que dicho sistema alberga o trata, determinarán la asignación de privilegios en el sistema. Esta asignación se debe hacer según el principio de menor privilegio, limitando los permisos únicamente a los estrictamente necesarios para la operativa de los usuarios.
    - De los servicios de red que presten. Los servicios de red que el sistema debe proveer
- deberán ser identificados, deshabilitando el resto de servicios. Por defecto, todo servicio que no se necesite y autorice deberá ser deshabilitado, habilitándose posteriormente sólo aquellos que se soliciten expresamente. En este sentido, deberá ser tratada con especial atención la supresión de servicios de comunicaciones que puedan ser utilizados por usuarios que se conecten de forma remota.
- El proceso de securización incluirá la instalación y configuración del software necesario para la detección de intrusiones en el sistema, disponiendo de los correspondientes registros.
- También, deberán controlarse de una manera segura los accesos a los puertos de diagnóstico remoto, con el fin de evitar accesos no autorizados, debiéndose proteger con un mecanismo de seguridad adecuado y permaneciendo sólo accesibles a solicitud de las personas encargadas del mantenimiento del hardware o del software.
- Para la definición de la configuración de seguridad, los equipos técnicos encargados harán un seguimiento de las vulnerabilidades publicadas en listas abiertas de distribución o a partir de los boletines de los fabricantes. En cualquier caso, se analizará el impacto de la vulnerabilidad anunciada y el impacto de variar la configuración de seguridad. Se deberá ser diligente con las actualizaciones de seguridad publicadas por los fabricantes con el objetivo de evitar ataques “0-day” o de “día 0”.
- Se mantendrá documentación actualizada relativa a las configuraciones

seguras de los sistemas. Esta documentación tendrá carácter confidencial.

6.18.- POLITICA DE EQUIPO DESANTENDIDO

Todos los equipos que permitan la característica, deben tener habilitados métodos de bloqueo automático después de cierto tiempo de inactividad, pudiendo desbloquear de nuevo el equipo utilizando algún método de autenticación de usuario. Esta característica debe funcionar de forma adecuada en los momentos en que se deja el equipo desatendido. En el caso que un equipo no tenga esta característica, no puede ser utilizado para manejar información confidencial de la organización, siendo obligatorio:

- El uso de contraseñas de usuario en equipos portátiles y teléfonos, usados para manipular información confidencial en la organización.
- El uso obligatorio de protectores de pantalla que bloquean el uso de equipos después de cierto tiempo de inactividad. El tiempo para iniciar el bloqueo no puede ser mayor a 15 minutos.

6.19.- POLITICA DE ESCRITORIO Y PANTALLA LIMPIA

Si el usuario de un equipo de información no se encuentra en su puesto de trabajo, se debe quitar toda la información sensible de la pantalla y escritorio y se debe denegar el acceso a todos los sistemas para los cuales la persona tiene autorización. En el caso de una ausencia corta (hasta 15 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas o bloqueando la pantalla con una clave.

Si la persona se ausenta por un período más prolongado (superior a 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas y apagando el puesto de trabajo, así como todos los documentos impresos, como también los soportes de almacenamiento de datos, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos. Este tipo de documentos y soportes deben ser archivados de forma segura, de acuerdo a lo establecido en la Política de Clasificación de la Información.

7.- RIESGOS DERIVADOS DEL TRATAMIENTO DE LOS DATOS PERSONALES

La gestión del riesgo es un elemento capital en los procesos de cualquier organización y es una parte inherente de la gestión de toda entidad, proyecto o actividad humana.

La gestión de riesgo está formada por un conjunto de acciones ordenadas y sistematizadas con el propósito de controlar las posibles (probabilidad) consecuencias (impactos) que una actividad puede tener sobre un conjunto de bienes o elementos (activos) que han de ser protegidos.

La gestión del riesgo precisa de un análisis, es decir, una reflexión crítica y objetiva de un tratamiento, requiere tomar decisiones que se han de plasmar en hechos concretos (controles) que minimicen el impacto sobre los activos hasta unos niveles tolerables.

El RGPD demanda la identificación, evaluación y mitigación, realizadas de una forma objetiva, del riesgo para los derechos y libertades de las personas en los tratamientos de datos personales. La mitigación ha de realizarse mediante la adopción de medidas técnicas y organizativas que garanticen y, además, permitan demostrar la protección de dichos derechos. Estás deberán determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento. Además, dichas medidas se revisarán y actualizarán cuando sea necesario. En definitiva, el RGPD exige un proceso de gestión del riesgo para los derechos y libertades de los interesados. En cumplimiento del principio de responsabilidad proactiva o “accountability”, la gestión del riesgo ha de estar documentada. Sin embargo, es importante saber diferenciar los informes que documentan las acciones de gestión del riesgo con la gestión del riesgo en sí misma. La gestión del riesgo no es un documento sino un proceso que se traduce en hechos y que se acredita documentalmente.

La Guía “**Gestión del Riesgo y Evaluación de Impacto en Tratamientos de Datos Personales**” se encuentra disponible en la Agencia Estatal de Protección de Datos y en el repositorio de guías en nuestro ERP.