POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

El presente documento contiene la POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN de **CELLA MEDICAL SOLUTIONS, S.L.**, en adelante la "organización".

La organización define, a través de este documento, una Política de Seguridad de la Información, de carácter obligatorio para todos aquellos comprendidos en el ámbito de aplicación, con el objetivo de 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.

Se recoge la información necesaria conforme al Artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Se desarrollan los siguientes aspectos:

1. Organización e implantación del proceso de seguridad.
2. Análisis y gestión de los riesgos.
3. Gestión de personal.
4. Profesionalidad.
5. Autorización y control de los accesos.
6. Protección de las instalaciones.
7. Adquisición de productos de seguridad y contratación de servicios de seguridad.
8. Mínimo privilegio.
9. Integridad y actualización del sistema.
10. Protección de la información almacenada y en tránsito.
11. Prevención ante otros sistemas de información interconectados.
12. Registro de actividad y detección de código dañino.
13. Incidentes de seguridad.
14. Continuidad de la actividad.
15. Mejora continua del proceso de seguridad.

La organización depende 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 daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar medidas de seguridad, así como realizar

un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación de los proyectos de TIC.

La Política está escrita a un nivel amplio, por lo que se complementará con documentos más precisos como normativas, procedimientos e instrucciones.

Cualquier plan específico sobre Seguridad de la Información deberá ajustarse a las disposiciones y recomendaciones, de carácter más general y superior de esta Política.

2. APROBACIÓN Y VIGENCIA

La presente política de seguridad de información entrará en vigor al día siguiente de su aprobación y estará vigente mientras que no se modifique.

Cualquier modificación a esta política requerirá la supervisión del Comité de Seguridad de la Información y aprobación la dirección general, previo a su entrada en vigor.

3. REVISIÓN

Anualmente será revisada la vigencia y razonabilidad de la Política de Seguridad de la Información por parte del Comité de Seguridad de la Información, así como del enfoque con el que se aborda la protección de la información.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad como a la adaptación a los cambios en el marco legal, infraestructura tecnológica, organización general, etc.

Entre los elementos a considerar se incluyen:

- Análisis y evaluación de riesgos.
- Resultados de auditorías o revisiones de terceros independientes o internas.
- Estado de las medidas preventivas o correctivas que pudieran estar planificadas.

- Análisis de cumplimiento por parte de terceros que prestan servicios a la organización.
- Tendencias asociadas a amenazas y vulnerabilidades.
- Información asociada a incidentes de seguridad identificados en la organización.
- Recomendaciones o directrices de órganos competentes.
- Cambios en el estándar adoptado como marco de referencia.

4. DIFUSIÓN Y CUSTODIA

La organización, a través del Comité de Seguridad de la Información, potenciará el conocimiento y difusión de la presente Política en los niveles adecuados, dado que interpreta este factor como crítico para asegurar su implantación eficaz y un cumplimiento efectivo.

Corresponde al Comité de Seguridad de la Información impulsar de forma efectiva la implantación de la Política de Seguridad de la Información.

Una vez aprobada y publicada, el original firmado o el fichero correspondiente validado por firma electrónica, quedará bajo la custodia del Responsable de Seguridad.

5. INCUMPLIMIENTO

El incumplimiento manifiesto de la Política de Seguridad de la Información por parte del personal de la organización o de terceros podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

6. ALCANCE

La presente Política aplica a todos los sistemas de información y al personal, a sus contratistas y a todos los que desarrollen funciones para la organización.

En particular, el acceso a los sistemas de información estará condicionado a la adhesión a esta Política y a los Procedimientos y Normativas asociados, siendo éstos de obligado cumplimiento.

7. OBJETIVOS

La Política de Seguridad de la Información velará por la seguridad de la información, siendo ésta de aplicación en todas las fases del ciclo de vida de la información y sus documentos: generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción; así como de los sistemas que los soportan: análisis, diseño, desarrollo, implantación, explotación y mantenimiento.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve la organización para desarrollar sus funciones, y se realicen, bajo garantías de seguridad, en sus distintas dimensiones: Disponibilidad; Integridad; Confidencialidad; Autenticidad; Trazabilidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la Información serán:

- Aceptar como activos estratégicos la información y los sistemas que la soportan garantizando su seguridad.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de contingencias y continuidad de la actividad que se definan.
- Realizar una adecuada gestión de incidentes 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.
- Adoptar la Política de Seguridad de la Información como la principal herramienta de garantía de seguridad de la información, promoviendo y asegurando su cumplimiento para todas las personas comprendidas en su ámbito de aplicación.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa legal vigente.

8. PRINCIPIOS

La Dirección de CELLA entiende su deber de garantizar la seguridad de la información como elemento esencial para el correcto desempeño de los servicios a sus clientes y, por tanto, soporta los siguientes principios:

I. Implementar el valor de la Seguridad de la Información en el conjunto de la Empresa.

II. Contribuir todas y cada una de las personas de CELLA a la protección de la Seguridad de la Información.

III. Preservar la confidencialidad, integridad y disponibilidad de la información, con el objetivo de garantizar que se cumplan los requisitos legales, normativos, y de los requisitos o exigencias de nuestros clientes, relativos a garantizar seguridad de la información.

IV. Proteger los activos de la información de CELLA de todas las amenazas, ya sean internas o externas, deliberadas o accidentales, con el objetivo de garantizar la continuidad del servicio ofrecido a nuestros clientes y la seguridad de la información que nos fuera confiada.

V. Establecer un plan de seguridad de la información que integre las actividades de prevención y minimización del riesgo de los incidentes de seguridad en base a los criterios de gestión del riesgo establecidos por CELLA.

VI. Proporcionar los medios necesarios para poder realizar las actuaciones pertinentes de cara a la gestión de los riesgos identificados.

VII. Definir como marco de gestión de la seguridad el compromiso de mejora continua utilizando como referencia la norma ISO/IEC 27001 para establecer el sistema de gestión de la seguridad de la información.

VIII. Adecuar las medidas de seguridad utilizando como referencia las guías de implantación de la norma ISO/IEC 27002 y de cualquier otra norma que pueda contribuir a la eficacia y eficiencia de la seguridad de la información y representen en “estado del arte” de la materia en todo momento.

IX. Asumir la responsabilidad en materia de concienciación y formación en materia de seguridad de la información como medio para garantizar el cumplimiento de esta política.

X. Extender el compromiso con la seguridad de la información a los clientes y beneficiarlos de la gestión diligente de la información como parte del compromiso de profesionalidad y responsabilidad de CELLA.

9. MARCO NORMATIVO

Según la legislación vigente, en el momento de aprobación de esta Política de Seguridad las leyes y normas aplicables a la organización en materia de Seguridad de la Información son:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (publicado en el BOE Nº 106, de 04/05/2022).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- UNE-EN ISO/IEC 27001:2017. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- 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 y por el que se deroga la Directiva 95/46/CE (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.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de Julio. De Servicios de Sociedad de la Información y de comercio electrónico.

10. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información de la organización son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones.

Para una mejor respuesta a incidentes de seguridad, la organización mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, proveedores de servicios informáticos o de comunicación, así como organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

En particular, la gestión de la seguridad de la información es responsabilidad específica de un conjunto de personas y comité con funciones concretas, definidas y documentadas

10.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información coordina la seguridad de la información en la organización. Éste está formado por los siguientes roles:

- Responsable de la información (RINF)
- Responsable del servicio (RSERV)
- Responsable de la seguridad (RSEG)
- Responsable de sistemas (RSIS)

10.2. FUNCIONES

10.2.1. Responsable de la información

El Responsable de la Información establecerá los requisitos sobre la información proporcionada a través de los servicios de la organización y, por tanto, tendrá la última palabra a la hora de decidir el tipo de información accesible y el uso que se le pueda dar, en virtud de la reglamentación vigente.

Le corresponden las siguientes funciones:

- Establecimiento de los requisitos de la información en materia de seguridad.
- Trabajo en colaboración con el Responsable de Seguridad y el Responsable de Sistemas en el mantenimiento de los sistemas.

Contará con la colaboración de los responsables de las unidades funcionales.

10.2.2. Responsable de los servicios

Le corresponden las siguientes funciones:

- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
- Es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Establecimiento de los requisitos de los servicios TIC en materia de seguridad.
- Trabajo en colaboración con el Responsable de Seguridad y el Responsable de Sistemas donde se englobe el/los servicios para el mantenimiento de los sistemas.

Contará con la colaboración de los responsables de las unidades funcionales.

10.2.3. Responsable de la seguridad

Le corresponden las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación de la Seguridad de la Información dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Aprobar toda la documentación relacionada con la seguridad de los sistemas.
- Verificar los informes de monitorización y auditoría de los estados de seguridad de los sistemas.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el Comité de Seguridad incluyendo los incidentes más relevantes del periodo.
- Aprobar de los procedimientos de seguridad cuando, en virtud del contenido, no requieran la aprobación del Comité de Seguridad.
- Proponer la redacción de aquella normativa de seguridad de la organización que considere necesario formalizar.
- Determinar la categorización de los sistemas y los requisitos de seguridad con carácter previo a la puesta en marcha de un nuevo servicio vinculado al ENS.

10.2.4. Responsable de sistemas

Sus funciones son las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Verificar la aplicación de los procedimientos operativos de seguridad en los sistemas de información.

- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para que la seguridad no esté comprometida y que en todo momento se ajusten a los procedimientos establecidos.
- Supervisar el estado de la seguridad de los sistemas.
- Informar al Responsable de Seguridad sobre cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
- Asesorar al Responsable de Seguridad para cumplir los requisitos de seguridad establecidos.

10.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Director General nombrará formalmente, mediante las resoluciones pertinentes al:

- Comité de Seguridad de la Información.
- Responsable de los Servicios.
- Responsable de la Información.
- Responsable del Sistema.
- Responsable de Seguridad.

Se seguirá el principio de seguridad como función diferenciada, de modo que:

- Responsable de Seguridad debe ser independiente del Responsable del Sistema.
- Responsable de Seguridad debe ser independiente de Responsables de los Servicios.
- Responsable de Seguridad debe ser independiente del Responsable de la Información.
- Responsable de los Servicios y de la Información puede ser la misma persona, pero debe ser independiente del Responsable del Sistema.

La asignación de roles y responsabilidades tendrá en cuenta la preceptiva segregación de funciones, de forma que las actuaciones de las personas titulares de los mismos no

comprometan la seguridad de Informaciones y Servicios en cualquiera de sus dimensiones (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad).

En casos excepcionales, sobre todo cuando no estén disponibles los recursos necesarios, pueden exceptuarse estas reglas de segregación de funciones, estableciendo las medidas compensatorias apropiadas para la resolución de los conflictos de intereses que puedan surgir.

10.4 RESOLUCIÓN DE CONFLICTOS

En caso de conflicto en materia de seguridad de la información entre los diferentes responsables y/o entre diferentes servicios de la organización, prevalecerá la decisión del Comité de Seguridad. Aquellos conflictos que no se resuelvan dentro del Comité de Seguridad se elevarán para decisión de la Dirección General.

11. DATOS DE CARÁCTER PERSONAL

Será de aplicación lo dispuesto en el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD).

Cada área o servicio se encargará de gestionar y mantener la seguridad referente a los datos de carácter personal incluidos en las operaciones de tratamiento que a tal efecto sean de su responsabilidad.

Las medidas de protección de los datos de carácter personal se establecerán a partir de los resultados del Análisis de Riesgos y de la Evaluación de Impacto prevista en el RGPD.

12. AUTORIZACIÓN Y CONTROL DE ACCESOS

La autorización de acceso a la información estará basada en la “necesidad de conocer”. Se autorizará el acceso a información clasificada como no pública, estrictamente a la persona que necesite conocer dicha información. La organización tomará las precauciones necesarias para que solo las personas autorizadas tengan acceso a los activos restringidos.

El acceso a los recursos, por parte de contratistas, está condicionado a la adhesión a la Política de Seguridad de la Información y a las Normativas asociadas existentes en la organización, siendo éstas de obligado cumplimiento.

Basado en un análisis de riesgos que atienda a la sensibilidad o criticidad de la información y los procesos que se llevan a cabo, se deberán proteger mediante controles más restrictivos aquellas zonas que presenten mayores riesgos (controles de acceso, protecciones ambientales, etc.). En cualquier caso, la protección suministrada deberá ser proporcional al riesgo y en función de la criticidad de la información.

La organización 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 deberá establecer las interfaces adecuadas entre la red interna y otras redes, los mecanismos adecuados de acceso y autenticación en el Sistema de Información para usuarios y equipos.

Los controles tendrán en cuenta, entre otros, las necesidades específicas de cada sistema, siendo el nivel de control coherente con la clasificación de la información gestionada; se hará uso de distintos perfiles de usuario que los sistemas operativos y aplicativos permitan y se tendrá en cuenta la segregación de funciones cuando se requiera; se seguirán los procedimientos de autorización, revocación y revisión de permisos y de gestión de contraseñas.

El uso de dispositivos móviles e instalaciones de trabajo remotas deberá disponer de las medidas necesarias para garantizar la seguridad de la información. La protección requerida será proporcional al riesgo que implique la modalidad del trabajo.

Se deberá monitorizar el adecuado funcionamiento de los controles implantados, mediante los reportes generados automáticamente, analizando los posibles accesos no autorizados y desviaciones respecto de la política de control de accesos.

13. PROTECCIÓN DE LAS INSTALACIONES

La información y los sistemas que la soportan, deberán ubicarse en áreas seguras adecuadamente protegidas de amenazas físicas o ambientales, ya sean estas intencionadas o accidentales. Será necesario establecer las suficientes garantías físicas de seguridad, a fin de reducir los riesgos de daños o pérdidas de datos.

Los sistemas o equipamiento de soporte a los procesos de información deberán estar protegidos razonablemente de potenciales amenazas del entorno (fuego, humedad, accidentes, etc.) y convenientemente de amenazas intencionadas (robo, copia, etc.).

14. MÍNIMO PRIVILEGIO

Los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.

Los sistemas se configurarán de forma que sean seguros por defecto, es decir, de forma que los usuarios realicen un uso seguro, salvo que conscientemente reduzcan la seguridad o se expongan a riesgos.

15. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento, para ello deben someterse a revisiones periódicas.

Los cambios y actualizaciones sobre los sistemas y tecnologías de la información estarán identificados y aprobados de forma previa a su puesta en explotación. En este sentido, los entornos de desarrollo y/o prueba estarán separados del entorno productivo o real para evitar incidentes que puedan afectar a la integridad y/o disponibilidad de la información.

16. GESTIÓN DE RIESGOS

El gobierno y la gestión de la seguridad de la información se guiarán por los resultados de los procesos de análisis y gestión de riesgos.

La reducción de los niveles de riesgo se realizará mediante la aplicación de controles. La selección y aplicación de los controles ponderarán el valor de los activos con los niveles de riesgo y el coste de la seguridad. Los controles deberán ser eficaces antes, durante o después de que ocurra un incidente de seguridad. Su objetivo es evitar que sucedan incidencias y controlar los daños si es que finalmente llegan a producirse.

17. REGISTRO DE ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO

Se definirá una estrategia global de monitorización de sistemas y actividades, identificando los sistemas más críticos y estableciendo los controles oportunos para registrar cualquier evento que debe ser detectado (actividades no autorizadas o funcionamientos inadecuados de sistemas). Los registros deberán ser almacenados convenientemente protegidos contra su modificación o eliminación.

Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento.

18. GESTIÓN DE INCIDENTES

Debe existir un procedimiento formal que considera los mecanismos para la identificación y escalado de incidentes, permitiendo una respuesta apropiada. Toda persona con acceso a los sistemas de información tiene la responsabilidad de reportar mediante los canales adecuados cualquier incidente o indicio que haya podido detectar.

19. CONTINUIDAD DE LA ACTIVIDAD

Debe existir un proceso de gestión de la continuidad de la operativa que permita la recuperación de los procesos y sistemas críticos. Con el fin de reducir el tiempo de indisponibilidad a niveles aceptables se combinarán controles de carácter organizativo, tecnológico y asociados a procedimientos, tanto preventivos como de recuperación.

En este sentido, estará disponible una infraestructura de respaldo que permita la recuperación de la operativa dentro de un marco temporal razonable a través de procedimientos, adecuadamente formalizados (incluyendo la asignación de responsabilidades), de invocación y recuperación.

Asimismo, y con carácter periódico, se revisará mediante verificaciones selectivas y/o parciales, la eficacia de las medidas planificadas para recuperar la operativa en caso de contingencia.

20. PROFESIONALIDAD

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

21. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Se usarán los siguientes instrumentos:

- Normas de seguridad: Uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.
- Procedimientos de seguridad: Afrontan tareas concretas, indicando lo que hay que hacer, paso a paso.

- Guías de seguridad: Tienen un carácter informativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos en los casos en los que no existan procedimientos precisos.

22. GESTIÓN DEL PERSONAL

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

Se establecerá un programa de acciones en concienciación continua para atender a todos los usuarios del sistema de información.

En su caso, si se requiere formación específica para el manejo seguro de los sistemas, las personas con responsabilidad en la operación o administración de sistemas TIC la recibirán en la medida en que la necesiten para realizar su trabajo.

23. CONTRATACIÓN Y ADQUISICIÓN DE PRODUCTOS

Cuando la organización utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que implique a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa.

Se deberá desarrollar un procedimiento de seguridad en relación con la gestión de proveedores donde se documentarán las consideraciones en materia de seguridad de la información en cuanto a la adquisición de nuevos componentes, la contratación de proveedores y la gestión de dichos contratos.

24. MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

Periódicamente se realizarán revisiones de los sistemas, normas y procedimientos con el fin de identificar oportunidades de mejora en la gestión de la seguridad y para la adaptación a los cambios en el marco legal, infraestructura tecnológica, organización general, etc.

Entre los elementos a considerar se incluyen:

- Análisis y evaluación de riesgos.
- Resultados de auditorías o revisiones de terceros independientes o internas.

- Estado de las medidas preventivas o correctivas que pudieran estar planificadas.
- Análisis de cumplimiento por parte de terceros que prestan los servicios en la organización.
- Tendencias asociadas a amenazas y vulnerabilidades.
- Información asociada a incidentes de seguridad identificados en la organización.
- Recomendaciones o directrices de órganos competentes.
- Cambios en el estándar adoptado como marco de referencia.

25. DOCUMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN

El nivel de calificación de la información de la organización se determina en función de los siguientes criterios:

- Valor de la información identificada.
- Criticidad de un incidente relacionado con la información de acuerdo con la evaluación de riesgos.
- Obligaciones legales y contractuales.

Se determinan tres niveles de calificación:

- Información PÚBLICA. La información está a disposición de cualquier persona.
- Información de USO INTERNO. La información está disponible para los usuarios de la organización con acceso al sistema de información.
- Información CONFIDENCIAL. La información está disponible únicamente para usuarios específicos en función de la necesidad de saber y los privilegios mínimos.

El responsable de cada información seguirá los criterios para asignar a cada información el nivel de seguridad requerido. Periódicamente se revisará la calificación de la información para evitar tanto una sobreprotección como una falta de protección.

26. CONFORMIDAD

El diseño, operación, uso y administración de los sistemas de información deberá estar sujeto a requisitos de seguridad legal, normativa y contractual. Se deberán impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

27. ÓRGANO RESOLUTOR

El órgano resolutor superior competente para todos los ámbitos será la dirección general.