# Política de Seguridad de la Información

## TABLA DE CONTENIDOS

## 1. INTRODUCCIÓN

La información, así como los medios para su tratamiento, transmisión y almacenamiento, constituye un activo enormemente valioso para todas las empresas de Grupo UCI.

Al mismo tiempo, el actual panorama tecnológico, caracterizado por un alto nivel de conectividad y acceso, dibuja un escenario donde los Sistemas de Información se encuentran sometidos a numerosos tipos de amenazas y riesgos que cada día van en aumento. Estas amenazas y riesgos afectan a las tres dimensiones fundamentales que caracterizan la Seguridad de la Información:

- Confidencialidad. La información asociada a los procesos de negocio de Grupo UCI debe ser única y exclusivamente accedida por las entidades autorizadas por Grupo UCI.
- Integridad. La información asociada a los procesos de negocio de Grupo UCI debe mantenerse exacta y completa.
- Disponibilidad. La información debe estar disponible cuando y como sea demandada por los procesos de negocio de Grupo UCI.

En consecuencia, se plantea la necesidad de proteger adecuadamente estos activos de forma que sea posible garantizar la continuidad de los procesos de negocio de Grupo UCI y minimizar los riesgos, al mismo tiempo que se maximiza el retorno de las inversiones.

Para garantizar la Seguridad de la Información, es necesario implantar y gestionar aquellos controles de Seguridad de la Información (Políticas, Normas, Procedimientos, mecanismos tecnológicos, etc.) que sean adecuados a las necesidades y requisitos de Grupo UCI.

El objeto del presente documento es establecer el marco conceptual sobre el que basar y desarrollar el proceso de Gestión de la Seguridad de la Información en Grupo UCI.

## 2. OBJETIVOS

La Dirección de Grupo UCI ha desarrollado la presente Política de Seguridad de la Información que establece el marco conceptual sobre el cual desarrollar el proceso de Gestión de la Seguridad de la Información. Dicho proceso de gestión de la seguridad se articula en torno a los siguientes objetivos:

- **OBJ01**. Identificar las necesidades de Grupo UCI en materia de Seguridad de la Información, expresadas en términos de Confidencialidad, Integridad y Disponibilidad.
- **OBJ02**. Gestionar los riesgos en Seguridad de la Información para que permanezcan dentro del Nivel de Riesgo Aceptable para Grupo UCI.
- **OBJ03**. Integrar el proceso de Gestión de Ciberincidentes con el Proceso de Continuidad de Negocio.
- **OBJ04**.Garantizar la adherencia al Marco Legal vigente en materia de Seguridad de la Información.

Por todo ello, la Dirección de Grupo UCI *declara explícitamente* su conocimiento y aprobación del presente documento, y lo publica de forma que todo el personal vinculado con la Organización tenga la obligación de conocerlo y de aplicarlo como parte de las tareas propias de su función, quedando las funciones de Seguridad de la Información integradas en todos los niveles jerárquicos del personal de Grupo UCI.

Para la aplicación efectiva de las Políticas de Seguridad de la información en la Compañía, la Dirección dotará de los recursos necesarios para su buen desarrollo, tanto en las actividades de implantación

como de mantenimiento de dichas Políticas y de los controles de seguridad que en cada momento se establezcan.

## 3. ALCANCE

Los requisitos definidos en la presente Política abarcan los Sistemas de Información e Infraestructuras Tecnológicas de Grupo UCI, así como la información corporativa, tanto si está en soporte informático como en otro tipo de soportes, siendo de obligado cumplimiento por todos los empleados, así como por aquellos terceros que hagan uso de la información de la Compañía, independientemente de su ubicación geográfica.

Asimismo, esta política se aplicará a las sucursales y filiales en el extranjero, aplicando las adaptaciones normativas que corresponda a cada país.

## 4. PRINCIPIOS DIRECTORES DE LA SEGURIDAD DE LA INFORMACIÓN

Grupo UCI establecerá los siguientes principios básicos como directrices fundamentales de Seguridad de la Información que han de tenerse siempre presentes en cualquier actividad relacionada con la información:

- Alcance estratégico. La Seguridad de la Información debe contar con el compromiso y apoyo de todos los niveles directivos de la Compañía de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas para conformar un todo coherente y eficaz.
- Alineación con las necesidades de negocio. Cualquier iniciativa en materia de seguridad de la información debe responder a requisitos y necesidades expuestas por los procesos y actividades de negocio de Grupo UCI.
- Seguridad integral. La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La Seguridad de la Información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los Sistemas de Información.
- Gestión de riesgos. El análisis y gestión de riesgos será parte esencial del proceso de Seguridad de la Información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta los niveles aceptables de riesgo formalmente definidos en Grupo UCI. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.
- Proporcionalidad. El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- Necesidad de conocer. El acceso a la información, así como los medios para su procesamiento, debe estar fundamentado en la necesidad para desarrollar una actividad vinculada con los procesos y objetivos de negocio de Grupo UCI.

- Obligación de conocer. Puesto que la Seguridad de la Información incumbe a todo el personal de Grupo UCI, esta Política deberá ser conocida, comprendida y asumida por todos sus empleados.
- Mínimo privilegio. Los usuarios recibirán solamente el nivel de permisos necesarios para llevar a cabo sus cometidos profesionales.
- Mejora continua. Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia y eficiencia a la constante evolución de los riesgos y sistemas de protección. La Seguridad de la Información será atendida, revisada y auditada por personal cualificado.
- Seguridad por defecto y mínima funcionalidad. Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto con la mínima funcionalidad imprescindible.
- Cumplimiento de la Normativa legal vigente. Cualquier iniciativa en materia de Seguridad de la Información debe cumplir estrictamente la Normativa legal vigente además de cumplir con las Políticas y Procedimientos internos de Grupo UCI.

# 5. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

## 5.1. GESTIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de Grupo UCI, así como todo el Cuerpo Normativo de Seguridad relacionado (Normas y Procedimientos) establecen los requisitos mínimos de Seguridad, que todos los departamentos de la Compañía deberán satisfacer en sus entornos.

Grupo UCI deberá considerar la Seguridad de la Información como una prioridad para la Organización y por ello, la presente Política establece las siguientes directrices:

- La información de la que Grupo UCI es propietaria y / o depositaria deberá ser únicamente accesible para las personas debidamente autorizadas, pertenezcan o no a la Compañía.
- La presente Política y su desarrollo deberán ser comunicados a todas las personas de Grupo UCI, tanto al personal propio como, en su caso, al personal externo del tercero contratado, y estar siempre a disposición de las partes interesadas. En el caso de personal externo, se realizarán las adaptaciones de la Política que apliquen en cada caso.
- Grupo UCI deberá cumplir con todos aquellos requerimientos legales, regulatorios y estatuarios que le sean de aplicación, así como con los requerimientos contractuales.
- La confidencialidad de la información deberá garantizarse en todo momento.
- La integridad de la información deberá asegurarse a través de todos los procesos que la gestionan o procesan y almacenan.
- La disponibilidad de la información deberá garantizarse mediante las medidas adecuadas de respaldo y continuidad de negocio.
- Todo el personal con responsabilidades en materia de Seguridad de la Información deberá disponer de la adecuada formación y concienciación.

- Todo incidente o debilidad que pueda comprometer o haya comprometido la confidencialidad, integridad y / o disponibilidad de la Información deberá ser registrado y analizado para aplicar las correspondientes medidas correctivas y / o preventivas.

Para la consecución de los objetivos de esta Política, Grupo UCI deberá establecer una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su reevaluación. En el transcurso de este ciclo de mejora continua, Grupo UCI mantendrá la definición tanto del nivel de riesgo residual aceptado (apetito de riesgo) como de sus umbrales de tolerancia.

### 5.2. ESTRUCTURA DEL CUERPO NORMATIVO DE SEGURIDAD

El Cuerpo Normativo de Seguridad deberá seguir una estructura jerárquica de documentos definida en tres niveles:

- Nivel 1. Política de Seguridad de la Información: se trata del presente documento, el cual es el principal del Cuerpo Normativo de Seguridad. Establece una declaración a alto nivel de objetivos y el compromiso de Grupo UCI para la gestión de la Seguridad de la Información. Los demás componentes del Cuerpo Normativo se basan y desarrollan a partir de esta Política.
- Nivel 2. Normas de Seguridad de la Información: conjunto de documentos que soportan los objetivos recogidos en la Política de Seguridad de Grupo UCI. En este nivel se detallan los requisitos de seguridad en un mayor nivel de detalle para cada sección o ámbito reflejado en la Política.
- Nivel 3. Procedimientos: estos documentos recogen el conjunto de tareas detalladas y especificadas con el fin de soportar la operativa diaria. Estas tareas están alineadas con los requisitos de seguridad establecidos en las Normas anteriores.

Las especificaciones y objetivos definidos en la Política de Seguridad junto con los requisitos establecidos en las diferentes Normas y Procedimientos de Seguridad que forman el Cuerpo Normativo de Seguridad de Grupo UCI serán de obligado cumplimiento por todos los empleados de la Compañía.

### 5.3. ASPECTOS ORGANIZATIVOS: ROLES Y FUNCIONES

La Seguridad de la Información deberá llevarse desde un entorno de gobierno y gestión (es decir, funciones y responsabilidades, segregación de funciones, contacto con las autoridades y grupos de interés especiales) y se deberá discutir la necesidad de establecer los requisitos de seguridad en Grupo UCI para la gestión de proyectos, la protección interna y la externalización de servicios.

Grupo UCI se compromete a velar por la Seguridad de todos los activos bajo su responsabilidad mediante las medidas que sean necesarias, siempre garantizando el cumplimiento de las distintas Normas y leyes aplicables.

Se acompaña el *Anexo I*, donde se detalla la composición de los equipos encargados de la definición, coordinación, mantenimiento y modificación de las Políticas de Seguridad de Grupo UCI. El *Anexo I* reflejará las actualizaciones necesarias al producirse cambios del personal involucrado.

### 5.4. GESTIÓN DE LA SEGURIDAD DE LOS RECURSOS HUMANOS

El departamento de Recursos Humanos deberá realizar su gestión teniendo en cuenta los criterios de seguridad establecidos en la Política de Seguridad, y dicho departamento representa un punto clave para asegurar el cumplimiento de la misma.

Las responsabilidades en materia de Seguridad deben ser consideradas en el proceso de selección de personal, en la elaboración de los contratos y durante la etapa laboral, a fin de reducir los riesgos de manipulación, robo, fraude o uso inadecuado de la Información.

Las obligaciones contractuales para los empleados se deberán reflejar en las Políticas y Normas de Seguridad de Grupo UCI. Los términos y condiciones deben incluir aspectos como acuerdos de confidencialidad, derechos legales, responsabilidades para el cumplimiento del Cuerpo Normativo y para el tratamiento de Información de terceros y acciones a tomar si la persona no cumple con los requisitos de Seguridad.

Todo el personal de la Compañía deberá recibir un nivel de formación y concienciación en materia de Seguridad de la Información. Por otro lado, es competencia de los empleados obrar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de terceros no autorizados. Asimismo, deberán ser informados de las actualizaciones de las Políticas y Normas de seguridad en los que se vean afectados y de las amenazas existentes de manera que pueda garantizarse el cumplimiento de esta Política.

### 5.5. GESTIÓN DE ACTIVOS

Grupo UCI deberá establecer un conjunto de medidas para organizar los activos de información, mantener su integridad y protegerlos de fugas, borrados accidentales o accesos no autorizados.

Toda la información de la Compañía deberá clasificarse para facilitar los procesos de control de acceso, custodia y monitorización. Sobre la base del nivel de clasificación de la información establecido, Grupo UCI deberá establecer medidas y controles preventivos, y cuanto más confidencial se considere la información, más restrictivos deberán ser dichos controles.

Asimismo, Grupo UCI deberá establecer las directrices de uso y manejo de dispositivos móviles (portátiles, teléfonos móviles, smartphones, tabletas, etc.), entre otros, suministrados por la Compañía y personales que hagan uso de sus sistemas de información. Al mismo tiempo, estará prohibido el almacenamiento de información propiedad de Grupo UCI en sistemas no corporativos y el uso de dispositivos personales se encontrará restringido y deberá ser analizado para evaluar el riesgo que podría introducir a la Compañía. En caso de aceptación, esta será registrada como excepción y se deberá hacer un seguimiento de la misma.

Por otro lado, el empleo y buen uso de tecnologías críticas (correo electrónico, Internet, redes sociales) deberá ser definido de cara a mantener una seguridad elevada y mitigar cualquier riesgo que pueda venir provocado debido a un mal uso de estas tecnologías.

### 5.6. CONTROL DE ACCESO

El acceso por parte del personal interno o externo a los sistemas o instalaciones de Grupo UCI, así como a la información o activos de los que se haga uso, se regulará sobre la base de las necesidades de información y operación de cada usuario, otorgando acceso exclusivamente a aquellas funciones e información que requieran para el correcto desempeño de su actividad laboral.

Los responsables de los activos serán los responsables de definir los niveles de acceso a los recursos y autorizar cualquier acceso extraordinario, así como de revisar regularmente los derechos de acceso de los usuarios.

Todos los accesos realizados a los Sistemas de Información de Grupo UCI llevarán asociado un proceso de identificación, autenticación y autorización, estableciéndose los controles necesarios para que tales procesos se realicen de forma segura.

Se deberán diseñar e implantar mecanismos de registro, monitorización de acceso y uso de los sistemas, que permitan conocer la efectividad de las medidas instaladas y detectar posibles incidentes de Seguridad.

De cara a garantizar estas medidas de seguridad, los usuarios deben ser únicos y no pueden ser compartidos, salvo excepciones debidamente autorizadas, evaluadas y documentadas. Todos ellos deben ser inicialmente asignados mediante el Principio de Mínimo Privilegio.

El acceso a aquellas instalaciones en las que se lleven a cabo procesos críticos para Grupo UCI deberá contar con un control adecuado de cara a minimizar el impacto en la continuidad operativa de los procesos de negocio, reduciendo el tiempo de indisponibilidad a los niveles establecidos.

### 5.7. CONTROLES CRIPTOGRÁFICOS

Grupo UCI deberá aplicar controles criptográficos sobre la base de la necesidad de implantar dichos controles en función del nivel de Seguridad requerido por la tipología de Información existente en los diferentes entornos y plataformas para garantizar la confidencialidad de la información.

Se deben alinear las medidas criptográficas con el esquema de clasificación de datos de Grupo UCI y se deberán desplegar mecanismos y herramientas de cifrado que sean inmunes a los ataques criptográficos más comunes.

Grupo UCI deberá implementar controles criptográficos en medios extraíbles que contengan información considerada como crítica según el esquema de clasificación de la Compañía, como es el caso de discos duros, portátiles, móviles, servidores y bases de datos.

Las claves de cifrado deberán ser almacenadas en aquellos sistemas corporativos destinados a dicho fin, ser adecuadamente protegidas y el acceso a las mismas solo debe estar permitido a través de un proceso estricto de autorización con el fin de preservar su confidencialidad. Del mismo modo, se deberá definir el periodo de vida de las claves de cifrado en el momento de su creación.

### 5.8. SEGURIDAD FÍSICA Y DEL ENTORNO

Los espacios físicos donde se ubican los sistemas de Información, así como los destinados al ámbito laboral de Grupo UCI, deberán estar adecuadamente protegidos. Asimismo, Grupo UCI deberá establecer medidas de Seguridad para proteger los activos físicos dentro y fuera del entorno laboral.

### 5.9. INFORMACIÓN EN SOPORTE NO DIGITAL O NO INFORMÁTICO

La presente Política es de aplicación también a la información propiedad de Grupo UCI que esté en formatos distintos del digital o informático, como es el caso de las copias impresas, las notas realizadas manualmente, las anotaciones realizadas en pizarras que quedan expuestas a la vista, etc.

En este sentido, Grupo UCI deberá tomar las medidas de seguridad necesarias para la protección de estas fuentes de información.

### 5.10. SEGURIDAD EN LA OPERATIVA

Todos los sistemas de Información de Grupo UCI deberán contar con las medidas de seguridad que optimicen el nivel de madurez de aquellos sistemas que se procesan o almacenan en la Entidad. Asimismo, se deberán gestionar y controlar las redes de manera adecuada, a fin de protegerse de las amenazas y mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluidos los controles de acceso, protegiendo así, toda la Información que se transfiera a través de estos elementos y / o entornos.

Se deberán establecer formalmente responsabilidades y Procedimientos documentados para asegurar una correcta configuración, administración, operación y monitorización de los Sistemas de Información de Grupo UCI. Para ello se deberá establecer la correspondiente Norma y se adoptarán las mejores prácticas en materia de seguridad.

Se deberán definir, planificar y realizar auditorías de forma periódica a los Sistemas de Información de Grupo UCI, con el objetivo de verificar el grado de cumplimiento de las distintas Normas y la efectividad de los controles aplicados a tal fin.

Dichas auditorias, dependiendo de la criticidad del activo de información en cuestión, pueden incluir actividades propias de hacking ético, detección de vulnerabilidades, pruebas de penetración o técnicas similares.

### 5.11. SEGURIDAD EN TRABAJO EN LA NUBE

El uso cada vez más intensivo por parte de Grupo UCI de modelos de trabajo en la Nube o Cloud Computing, incorpora riesgos concretos para la Seguridad de la Información que es preciso controlar específicamente. Por lo tanto, Grupo UCI deberá mantener una Norma de Seguridad en la Nube que establezca las medidas de seguridad adecuadas para garantizar la confidencialidad, integridad y disponibilidad de su información, teniendo en cuenta que la responsabilidad sobre la información y los activos sigue recayendo sobre la Compañía.

### 5.12. SEGURIDAD EN LAS TELECOMUNICACIONES

La Información transmitida por redes de comunicaciones, públicas o privadas, deberá ser adecuadamente protegida mediante mecanismos de seguridad que garanticen su confidencialidad, disponibilidad e integridad. Se deberán 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 entidades con las que Grupo UCI tenga relación.

Las arquitecturas de redes de Grupo UCI deberán contar con medidas de prevención, detección y respuesta para evitar brechas en los dominios internos y externos, siendo de suma importancia la administración de seguridad de las redes que atraviesan el perímetro de Grupo UCI, implantando controles adicionales para los datos sensibles que circulen por las redes de comunicación públicas.

Siempre que tecnológicamente sea posible, se deberá realizar una segregación entre las redes de datos y red de seguridad, de cara a preservar la integridad de la información que circula por ellas.

En cuanto a la conexión remota a las redes de Grupo UCI, se debe establecer un conjunto de tecnologías y controles de seguridad según el perfil de usuario.

Los riesgos asociados a las redes inalámbricas tendrán el mismo tratamiento que los riesgos correspondientes a las redes cableadas, teniendo en cuenta las peculiaridades de ambos tipos de redes.

### 5.13. SEGURIDAD EN EL CICLO DE VIDA DEL DESARROLLO DE SISTEMAS

Los requisitos de seguridad deberán ser considerados durante todo el Ciclo de Vida de Desarrollos y de Infraestructuras Tecnológicas de Grupo UCI, tanto en sistemas de desarrollo propio como en aquellos desarrollados por terceros, desde las fases de análisis de requerimientos y viabilidad, en las que se particularizan y evalúan dichos requisitos, a las fases de diseño, pruebas, implantación, aceptación y su posterior mantenimiento.

Para el correcto desarrollo de software, se deberá disponer de un plan de pruebas de seguridad que incluye revisiones de código seguro, protección de datos, etc. Asimismo, se deberán realizar pruebas de penetración y escaneo de vulnerabilidades sobre todo desarrollo de software antes de su paso a producción.

Cada unidad de negocio de Grupo UCI deberá tener en cuenta la Seguridad de la Información en sus procesos y procedimientos de selección, desarrollo e implementación de aplicaciones, productos y servicios.

Grupo UCI deberá realizar comunicaciones a los desarrolladores de sistemas sobre las Normas de seguridad y sus objetivos, así como otras Normativas aplicables.

### 5.14. SEGURIDAD EN LOS PROVEEDORES

Grupo UCI deberá poner especial atención en evaluar la criticidad de todos los servicios susceptibles de ser subcontratados de manera que puedan identificarse aquellos que sean relevantes desde el punto de vista de la Seguridad de la Información, ya sea por su naturaleza, la sensibilidad de los datos que deban tratarse o la dependencia sobre la continuidad del negocio.

Sobre los proveedores de estos servicios se deberán cuidar los procesos de selección, requerimientos contractuales, la monitorización de los niveles de servicio y las medidas de seguridad implantadas por dicho proveedor. Siendo obligatoria la presentación de evidencias sobre el buen estado del proveedor en materia de cumplimiento con legislación fiscal y laboral, y revisándose como mínimo anualmente.

Se deberá disponer de procesos formales para la finalización de la relación con los proveedores, que incluyan cláusulas contractuales específicas para asegurar la privacidad y el retorno o eliminación de la Información una vez finalizado el servicio.

### 5.15. GESTIÓN DE CIBERINCIDENTES

Todos los empleados de Grupo UCI tienen la obligación y responsabilidad de la identificación y notificación al responsable de Ciberseguridad de la Compañía de cualquier incidente o delito que pudiera comprometer la seguridad de sus activos de información. Asimismo, Grupo UCI deberá implementar Procedimientos para la correcta gestión de los incidentes detectados.

Grupo UCI deberá disponer de un proceso de respuesta ante incidentes para gestionar de forma correcta todas las amenazas materializadas en la Organización. Este proceso incluye aspectos como la monitorización, seguimiento, clasificación y remediación de dichos incidentes.

Todo incidente que pueda comprometer o haya comprometido la confidencialidad, integridad y / o disponibilidad de la Información deberá ser registrado y analizado para aplicar las correspondientes medidas correctivas y / o preventivas.

Se deberá establecer un plan de simulaciones que ayuden al entrenamiento y concienciación del personal de la Entidad.

### 5.16. CONTINUIDAD DE NEGOCIO

Respondiendo a requerimientos de calidad y buenas prácticas, Grupo UCI deberá disponer de un Plan de Continuidad de Negocio como parte de su estrategia para garantizar la continuidad en la prestación de sus servicios vitales y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para que la Compañía actúe en caso de ser necesario. Este Plan de Continuidad deberá ser revisado y probado periódicamente.

En el desarrollo de este plan se debe considerar no solo el plan de contingencia de Sistemas de Información, sino también de los propios Servicios de Seguridad, las dependencias físicas, las personas que dan soporte a la actividad de negocio y los recursos que puedan necesitar para que la Organización pueda seguir desarrollando su actividad productiva y de atención hacia los clientes.

El plan de contingencia se debe desarrollar e implementar para asegurar que los procesos críticos de negocio puedan restablecerse en el tiempo requerido, incluyendo controles para identificar y reducir los riesgos, limitar las consecuencias de los incidentes que afectan negativamente, y asegurar el tiempo de respuesta de las operaciones esenciales. Dentro de este plan son partes fundamentales la formación a los componentes del equipo de gestión de crisis, así como el ejercicio de ensayo y verificación regular sobre los planes de respuesta definidos.

El plan ha de ser revisado y publicado como mínimo una vez al año o cuando por causas suficientes sufra de cambios importantes, como nuevos activos inmobiliarios, tecnológicos, organizativo.

Toda la Información sensible, confidencial o datos de carácter personal deben estar registrada en copias de respaldo. La gestión de estas copias de Seguridad se debe realizar y conservar de acuerdo con las medidas de Seguridad definidas por Grupo UCI.

### 5.17. CUMPLIMIENTO NORMATIVO Y LEGAL

Grupo UCI se compromete a dotar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a la actividad de la Compañía en materia de Seguridad de la Información y establece la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se velará por el cumplimiento de toda legislación, Normativa o regulación aplicable.

Con el fin de asegurar la confidencialidad, la integridad y disponibilidad de la información, y detectar posibles incumplimientos, los sistemas de Grupo UCI estarán sujetos a la realización periódica de actividades de auditoría y monitorización.

### 5.18. GESTIÓN DE EXCEPCIONES

Cualquier excepción al Cuerpo Normativo de Seguridad deberá ser registrada e informada al Comité de Ciberseguridad de Grupo UCI, así como aprobadas por el mismo. Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir a la Compañía y, en base a la categorización de estos riesgos, estos deberán ser asumidos por el peticionario de la excepción junto con los responsables del negocio. Se deberá realizar un seguimiento a dichas excepciones.

### 5.19. SANCIONES DISCIPLINARIAS

Cualquier violación de la presente Política de Seguridad puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el *Procedimiento Disciplinario* de Grupo UCI. Es responsabilidad de todos los miembros de Grupo UCI notificar al Responsable de Ciberseguridad cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política, conforme se recoge en el epígrafe 5.15 *Gestión de Ciberincidentes* de este mismo documento.

## 6. GOBIERNO DE LA POLÍTICA DE SEGURIDAD

La presente Política de Seguridad de la Información, será revisada y aprobada anualmente por parte del Comité de Ciberseguridad de Grupo UCI. No obstante, si tuvieran lugar cambios relevantes en la Compañía o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento a la realidad de la Compañía.

Las propuestas de modificación o adaptación serán aceptadas y validadas por el Comité de Ciberseguridad.

## 7. REFERENCIAS EXTERNAS E INTERNAS

Los marcos legales y regulatorios de aplicación, así como las referencias consultivas en materia de Seguridad de la Información se hallan recogidas en epígrafe 9 *REFERENCIAS EXTERNAS E INTERNAS* de la Norma *UCI.SGSI.NOR1800.Cumplimiento.Regulatorio.Legal*.

## 8. ANEXO I: ENCARGADOS DE LA COORDINACIÓN DE LA POLÍTICA DE SEGURIDAD

| Equipo/Rol | Responsabilidades |
|---|---|
| Comité de Ciberseguridad | Aprobación y coordinación. Coordina la Seguridad de la Información en la Compañía. Estará formado por miembros del Comité de Dirección, por el Responsable de Ciberseguridad y por representantes de otras áreas de Grupo UCI. |
| Responsable de Ciberseguridad | Encargado de Seguridad de la Información. Este cargo lo ocupa el CISO de Grupo UCI: Enrique Aristi. |
| Responsable del Servicio | Encargado de establecer los requisitos de un servicio en materia de seguridad. |
| Usuarios | Aplicar y cumplir. |

*Nota: Esta información debe ser actualizada cuando ocurran modificaciones en los actores miembros de los equipos encargados de la coordinación. Los requisitos detallados se desarrollan en el Procedimiento de Modelo de Gobierno de Seguridad.*