Política de Seguridad de la Información

Febrero 2026

Índice de contenidos

1. Cambios con respecto a la versión anterior

Se actualizan los objetivos de la Política de Seguridad de la Información, con el propósito de fortalecer la postura de seguridad y garantizar la mejora continua del sistema de gestión. Se indican los cambios en el Rol de CISO y Responsable de Ciberseguridad.

2. 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.

3. Objeto

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. Gobierno, cumplimiento y mejora continua de la Seguridad de la Información.** Establecer y mantener un modelo de gobierno sólido de la Seguridad de la Información que permita garantizar la adherencia al marco Legal vigente en materia de Seguridad de la Información, así como la mejora continua del sistema de gestión mediante auditorías, revisiones periódicas y la actualización del Cuerpo Normativo de Seguridad de UCI y de la documentación referente a Continuidad de Negocio.
- **OBJ02. Gestión del riesgo tecnológico.** Asegurar una gestión actualizada del riesgo de ciberseguridad, identificando, evaluando y tratando los riesgos que puedan afectar a la confidencialidad, integridad o disponibilidad de los activos de información, incluyendo los riesgos criptográficos y simulaciones operativas.
- **OBJ03. Medición, control y madurez en ciberseguridad.** Proporcionar mecanismos de medición eficaces que permitan conocer, evaluar y comunicar el estado de la ciberseguridad mediante indicadores clave, cuadros de mando e informes de madurez en ciberseguridad.
- **OBJ04. Capacitación y formación.** Se deberá impulsar una cultura de ciberseguridad transversal en toda la organización, asegurando que empleados externos e internos dispongan del conocimiento necesario para proteger la información de acuerdo a sus responsabilidades, al tiempo que se deben reforzar las capacidades especializadas de los equipos que trabajen directamente en la Seguridad de la Información.
- **OBJ05. Protección de la Información.** Garantizar que la información de Grupo UCI recibe un nivel de protección adecuado durante todo su ciclo de vida, mediante el cifrado, monitorización e identificación proactiva de datos sensibles, reduciendo su riesgo de fuga, acceso no autorizado o uso indebido de la información.
- **OBJ06. Protección de dispositivos de usuario.** Asegurar la protección de los dispositivos de usuario, tanto en entornos corporativos como de teletrabajo y movilidad, mediante el control centralizado, la gestión de configuraciones seguras y la reducción de superficies de ataque derivadas del uso de tecnologías no autorizadas.
- **OBJ07. Bastionado y protección de infraestructuras tecnológicas.** Garantizar que las infraestructuras tecnológicas, tanto de sistemas operativos como de red y plataformas corporativas, se encuentren correctamente bastionadas y configuradas de acuerdo con buenas prácticas de seguridad, reduciendo vulnerabilidades y evitando configuraciones inseguras en entornos productivos.
- **OBJ08. Protección de aplicaciones y servicios expuestos.** Asegurar la protección

de las aplicaciones corporativas y de los servicios expuestos a Internet frente a amenazas externas, mediante mecanismos de defensa que permitan prevenir, detectar y mitigar ataques dirigidos a capas de aplicación.

- **OBJ09. Gestión y control de activos de información.** Disponer de un inventario actualizado, fiable y centralizado de los activos tecnológicos y de información.
- **OBJ10. Detección, respuesta y orquestación de ciberincidentes.** Proporcionar capacidades avanzadas de detección, respuesta y automatización frente a ciberincidentes, permitiendo una actuación rápida, coordinada y eficiente ante amenazas, minimizando el impacto sobre la operación y la información.
- **OBJ11. Inteligencia de amenazas y gestión de vulnerabilidades.** Fortalecer la postura de seguridad de Grupo UCI mediante la identificación continua de vulnerabilidades y el análisis del contexto de amenazas, anticipándose a posibles ataques.

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.

4. Ámbito de aplicación

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 aplica a las sucursales y filiales en el extranjero, aplicando las adaptaciones normativas que corresponda a cada país.

De acuerdo con los principios generales establecidos en el Procedimiento de Gobernanza de Marcos y Políticas**, los cambios no significativos** de la presente política **podrán ser validados por el Comité de Dirección**, con la obligación de informar a la Comisión Independiente de Auditoría y Riesgos / Consejo de Administración. Por su parte, **los cambios significativos deberán ser validados por la Comisión Independiente de Auditoría y Riesgos / Consejo de Administración**, debiendo informarse al Comité de

Dirección. En cualquier caso, la presente política se revisará y actualizará cada tres años.

5. Definiciones

Los términos, conceptos y definiciones incluidos en esta Norma se pueden encontrar en el documento:
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

6. Referencias

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*.

7. 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 las 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 entiende 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 es considerada 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 es 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 realiza mediante el despliegue de medidas de seguridad, que establecen 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 debe ser conocida, comprendida y asumida por todos sus empleados.
- Mínimo privilegio. Los usuarios reciben solamente el nivel de permisos necesarios para llevar a cabo sus cometidos profesionales.
- Mejora continua. Las medidas de seguridad se reevalúan y actualizan 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.

8. Desarrollo de la Política de Seguridad

8.1 Gestión de la Política de Seguridad de la Información

La presente Política de Seguridad de Grupo UCI, será revisada y aprobada anualmente por parte del Consejo de Dirección de 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.

8.2 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 considera 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 es 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.

8.3 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.
  Aunque no recogidos en el Cuerpo Normativo de Seguridad, cabe indicar la existencia de documentos Procedimentales, los cuales 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 correspondientes. La Normas que desarrollas la Política de Seguridad de la Información se hallan inventariadas en el documento *UCI.SGSI.NOR0000.Norma.Cero*.

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

8.4 Aspectos Organizativos: Roles y Responsabilidades

La Seguridad de la Información se lleva 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 establece la necesidad de establecer los requisitos de seguridad en Grupo UCI para la gestión de proyectos, la protección interna y la externalización de servicios.

El 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.

8.5 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 esta.

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 recibe 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, son 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.

8.6 Gestión de Activos

Grupo UCI establece 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 se clasifica para facilitar los procesos de control de acceso, custodia y monitorización. Sobre la base del nivel de clasificación de la información establecido, Grupo UCI establece medidas y controles preventivos, y cuanto más confidencial se considere la información, más restrictivos son dichos controles.

Asimismo, Grupo UCI establece 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 encuentra 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 esta.

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

8.7 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, está regulado 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 son 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 llevan asociados un proceso de identificación, autenticación y autorización, estableciéndose los controles necesarios para que tales procesos se realicen de forma segura.

Existen 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 son únicos y no pueden ser compartidos, salvo excepciones debidamente autorizadas, evaluadas y documentadas. Todos ellos son 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 cuenta 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.

8.8 Controles Criptográficos

Grupo UCI aplica 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 alinean las medidas criptográficas con el esquema de clasificación de datos de Grupo UCI y se despliegan mecanismos y herramientas de cifrado que son inmunes a los ataques criptográficos más comunes.

El Grupo UCI implementa 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 son 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 define el periodo de vida de las claves de cifrado en el momento de su creación.

8.9 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, están adecuadamente protegidos. Asimismo, Grupo UCI establece medidas de Seguridad para proteger los activos físicos dentro y fuera del entorno laboral.

8.10 Información en Soporte no Digital o no Informático

La presente Política es de aplicación también a la información propiedad de Grupo UCI que está 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 toma las medidas de seguridad necesarias para la protección de estas fuentes de información.

8.11 Seguridad en la Operativa

Todos los sistemas de Información de Grupo UCI cuentan 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 establecen 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 debe seguir la correspondiente Norma y se adoptarán las mejores prácticas en materia de seguridad.

Se definen, planifican y realizan 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.

8.12 Seguridad en el 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 mantiene 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.

8.13 Seguridad en las Telecomunicaciones

La Información transmitida por redes de comunicaciones, públicas o privadas, está adecuadamente protegida mediante mecanismos de seguridad que garanticen su confidencialidad, disponibilidad e integridad. Se establecen 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 cuentan 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 establece 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.

8.14 Seguridad en el ciclo de vida de los 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 realizan 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 realiza comunicaciones a los desarrolladores de sistemas sobre las Normas de seguridad y sus objetivos, así como otras Normativas aplicables.

8.15 Seguridad en los Proveedores

Grupo UCI pone 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 cuidan 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 tanto de seguridad como de cumplimiento con legislación fiscal y laboral, y se revisa periódicamente en base a la categorización del riesgo de cada proveedor

Score riesgo	Plazo/años
Bajo / Medio-Bajo	3
Medio-alto	2
Alto	1
Externalizaciones esenciales	1

Se dispone 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.

8.16 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 tiene implementados Procedimientos para la correcta gestión de los incidentes detectados.

Grupo UCI dispone 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 ha establecido un plan de simulaciones que ayuden al entrenamiento y concienciación del personal de la Entidad.

8.17 Continuidad de Negocio

Respondiendo a requerimientos de calidad y buenas prácticas, Grupo UCI dispone 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 considera 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 desarrolla e implementa para asegurar que los procesos críticos de negocio puedan restablecerse en el tiempo requerido, incluyendo controles para identificar y reducir los riesgos, limitando las consecuencias de los incidentes que afectan negativamente, y asegurando 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 está registrada en copias de respaldo. La gestión de estas copias de Seguridad se realiza y conserva de acuerdo con las medidas de Seguridad definidas por Grupo UCI.

8.18 Cumplimiento Normativo 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

8.19 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.

8.20 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 8.16 Gestión de Ciberincidentes de este mismo documento.

9. Anexos

9.1 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, CISO y por representantes de otras áreas de Grupo UCI.
CISO	Encargado de Seguridad de la Información. Este cargo lo ocupa el CISO de Grupo UCI: David Espantaleón
Responsable de Ciberseguridad	Encargado de Seguridad de la Seguridad Operativa de la compañía. Este cargo lo ocupa David Paños
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.

10. Alterações em relação à versão anterior

São atualizados os objetivos da Política de Segurança da Informação, com o propósito de fortalecer a postura de segurança e garantir a melhoria contínua do sistema de gestão.

11. Introdução

A informação, bem como os meios para o seu tratamento, transmissão e armazenamento, constitui um ativo bastante valioso para todas as empresas do Grupo UCI.

Ao mesmo tempo, o atual panorama tecnológico, caracterizado por um alto nível de conectividade e acesso, desenha um cenário em que os Sistemas de Informação estão sujeitos a vários tipos de ameaças e riscos que cada dia vão aumentando. Estas ameaças e riscos dizem respeito às três dimensões fundamentais que caracterizam a Segurança da Informação:

- Confidencialidade. A informação associada aos processos comerciais do Grupo UCI deve ser única e exclusivamente acedida pelas entidades autorizadas pelo Grupo UCI.
- Integridade. A informação associada aos processos comerciais do Grupo UCI deve manter-se exata e completa.
- Disponibilidade. A informação deve estar disponível quando e conforme seja solicitada pelos processos comerciais do Grupo UCI.

Consequentemente, coloca-se a necessidade de proteger adequadamente estes ativos para que seja possível garantir a continuidade dos processos comerciais do Grupo UCI e minimizar os riscos, ao mesmo tempo que se maximiza o retorno dos investimentos.

Para garantir a Segurança da Informação, é necessário implementar e gerir os controlos de Segurança da Informação (Políticas, Normas, Procedimentos, mecanismos tecnológicos, etc.) que sejam adequados às necessidades e requisitos do Grupo UCI.

O objetivo do presente documento é estabelecer o quadro conceptual sobre o qual se deve basear e desenvolver o processo de Gestão da Segurança da Informação no Grupo UCI.

12. Objetivo

A Administração do Grupo UCI desenvolveu a presente Política de Segurança da Informação, que estabelece o quadro conceptual sobre o qual se deve desenvolver o processo de Gestão da Segurança da Informação. Esse processo de gestão da segurança articula-se em torno dos seguintes objetivos:

- **OBJ01. Governança, conformidade e melhoria contínua da Segurança da**

Informação. Estabelecer e manter um modelo sólido de governança da Segurança da Informação que assegure a conformidade com o marco legal vigente na matéria, bem como a melhoria contínua do sistema de gestão por meio de auditorias, revisões periódicas e da atualização do Corpo Normativo de Segurança da UCI e da documentação relacionada à Continuidade de Negócios.

- **OBJ02. Gestão do risco tecnológico.** Assegurar uma gestão atualizada dos riscos de cibersegurança, identificando, avaliando e tratando os riscos que possam afetar a confidencialidade, integridade ou disponibilidade dos ativos de informação, incluindo riscos criptográficos e simulações operacionais.
- **OBJ03. Medição, controle e maturidade em cibersegurança.** Disponibilizar mecanismos de medição eficazes que permitam conhecer, avaliar e comunicar o estado da cibersegurança por meio de indicadores-chave, painéis de controle e relatórios de maturidade em cibersegurança.
- **OBJ04. Capacitação e formação.** Promover uma cultura transversal de cibersegurança em toda a organização, assegurando que colaboradores internos e externos possuam o conhecimento necessário para proteger a informação de acordo com suas responsabilidades, ao mesmo tempo em que se reforçam as competências especializadas das equipes que atuam diretamente na Segurança da Informação.
- **OBJ05. Proteção da Informação.** Garantir que as informações do Grupo UCI recebam um nível adequado de proteção durante todo o seu ciclo de vida, por meio de criptografia, monitoramento e identificação proativa de dados sensíveis, reduzindo o risco de vazamento, acesso não autorizado ou uso indevido das informações.
- **OBJ06. Proteção de dispositivos do usuário.** Assegurar a proteção dos dispositivos de usuário, tanto em ambientes corporativos quanto em cenários de teletrabalho e mobilidade, por meio de controle centralizado, gestão de configurações seguras e redução das superfícies de ataque decorrentes do uso de tecnologias não autorizadas.
- **OBJ07. Endurecimento e proteção de infraestruturas tecnológicas.** Garantir que as infraestruturas tecnológicas, incluindo sistemas operacionais, redes e plataformas corporativas, estejam devidamente protegidas (hardening) e configuradas de acordo com as boas práticas de segurança, reduzindo vulnerabilidades e evitando configurações inseguras em ambientes produtivos.
- **OBJ08. Proteção de aplicações e serviços expostos.** Assegurar a proteção das aplicações corporativas e dos serviços expostos à Internet contra ameaças externas, por meio de mecanismos de defesa que permitam prevenir, detectar e mitigar ataques direcionados às camadas de aplicação.
- **OBJ09. Gestão e controle de ativos de informação.** Manter um inventário atualizado, confiável e centralizado dos ativos tecnológicos e de informação.
- **OBJ10. Detecção, resposta e orquestração de ciberincidentes.** Disponibilizar capacidades avançadas de detecção, resposta e automação frente a ciberincidentes, permitindo uma atuação rápida, coordenada e eficiente diante de ameaças, minimizando o impacto sobre as operações e as informações.
- **OBJ11. Inteligência de ameaças e gestão de vulnerabilidades.** Fortalecer a

postura de segurança do Grupo UCI por meio da identificação contínua de vulnerabilidades e da análise do contexto de ameaças, antecipando-se a possíveis ataques.

Por tudo isso, a Administração do Grupo UCI declara expressamente o seu conhecimento e aprovação do presente documento, e publica-o de forma que todo o pessoal vinculado à Organização tenha a obrigação de o conhecer e aplicar como parte das tarefas próprias da sua função, ficando as funções de Segurança da Informação integradas em todos os níveis hierárquicos do pessoal do Grupo UCI.

Para a implementação efetiva das Políticas de Segurança da Informação na Sociedade, a Administração proporcionará os recursos necessários para o seu bom desenvolvimento, tanto nas atividades de implementação como de manutenção dessas Políticas e dos controlos de segurança que em cada momento sejam estabelecidos.

13. Âmbito de aplicação

Os requisitos definidos na presente Política abrangem os Sistemas de Informação e Infraestruturas Tecnológicas do Grupo UCI, bem como a informação societária, tanto se estiver em suporte informático como em outro tipo de suportes, sendo de cumprimento obrigatório por todos os funcionários, bem como pelos terceiros que façam uso da informação da Sociedade, independentemente da sua localização geográfica.

Do mesmo modo, esta política aplica-se às sucursais e filiais no estrangeiro, aplicando as adaptações normativas que digam respeito a cada país.

De acordo com os princípios gerais estabelecidos no Procedimento de Governação de Marcos e Políticas, **as alterações não significativas** à presente política **poderão ser validadas pelo Comité de Direção**, com a obrigação de informar a Comissão Independente de Auditoria e Riscos / Conselho de Administração. Por sua vez, **as alterações significativas deverão ser validadas pela Comissão Independente de Auditoria e Riscos / Conselho de Administração**, devendo ser comunicado ao Comité de Direção. Em qualquer dos casos, a presente política será revista e atualizada a cada três anos.

14. Definições

Os termos, conceitos e definições incluídos nesta Norma podem ser encontrados no documento:
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2

021.pdf

15. Referências

Os quadros legais e regulamentares que sejam aplicáveis, bem como as referências consultivas em matéria de Segurança da Informação estão reunidas na secção 9 *REFERÊNCIAS EXTERNAS E INTERNAS* da Norma *UCI.SGSI.NOR1800.Cumprimento.Regulamentar.Legal*.

16. Princípios orientadores da Segurança da Informação

O Grupo UCI estabelece os seguintes princípios básicos como orientações fundamentais da Segurança da Informação que devem estar sempre presentes em qualquer atividade relacionada com a informação:

- Alcance estratégico. A Segurança da Informação deve contar com o compromisso e apoio de todos os níveis dirigentes da Sociedade, para que possa estar coordenada e integrada com o resto das iniciativas estratégicas para formar um todo coerente e eficaz.
- Alinhamento com as necessidades comerciais. Qualquer iniciativa em matéria de segurança da informação deve responder a requisitos e necessidades reveladas pelos processos e atividades comerciais do Grupo UCI.
- Segurança integral. A segurança da informação considera-se um processo integral constituído por elementos técnicos, humanos, materiais e organizativos, evitando, salvo em casos de urgência ou necessidade, qualquer atuação pontual ou tratamento conjuntural. A Segurança da Informação considera-se como fazendo parte da operação habitual, estando presente e aplicando-se desde a conceção inicial dos Sistemas de Informação.
- Gestão de riscos. A análise e gestão de riscos é parte essencial do processo de Segurança da Informação. A gestão de riscos permitirá a manutenção de um ambiente controlado, minimizando os riscos até níveis aceitáveis de risco formalmente definidos no Grupo UCI. A redução destes níveis realiza-se através da implementação de medidas de segurança, que estabeleçam um equilíbrio entre a natureza dos dados e os tratamentos, o impacto e a probabilidade dos riscos a que estão expostos e a eficácia e o custo das medidas de segurança.
- Proporcionalidade. O estabelecimento de medidas de proteção, deteção e recuperação deve ser proporcional aos potenciais riscos e à criticidade e valor da informação e dos serviços afetados.
- Necessidade de conhecer. O acesso à informação, bem como os meios para o seu processamento, deve tem como fundamento a necessidade para desenvolver uma atividade associada aos processos e objetivos comerciais do Grupo UCI.

- Obrigação de conhecer. Como a Segurança da Informação é da responsabilidade de todo o pessoal do Grupo UCI, esta Política deve ser conhecida, compreendida e assumida por todos os seus funcionários.
- Privilégio mínimo. Os utilizadores recebem apenas o nível de autorizações necessárias para levar a cabo as suas tarefas profissionais.
- Melhoria contínua. As medidas de segurança são reavaliadas e atualizadas periodicamente para adequar a sua eficácia e eficiência à constante evolução dos riscos e sistemas de proteção. A Segurança da Informação será considerada, revista e auditada por pessoal qualificado.
- Segurança por defeito e mínima funcionalidade. Os sistemas devem ser concebidos e configurados de forma a garantir um grau suficiente de segurança por defeito, com a mínima funcionalidade imprescindível.
- Cumprimento da Normativa legal vigente. Qualquer iniciativa em matéria de Segurança da Informação deve cumprir estritamente a Normativa legal vigente, além de cumprir as Políticas e Procedimentos internos do Grupo UCI.

17. Desenvolvimento da Política de Segurança

17.1 Governo da Política de Segurança da Informação

A presente Política de Segurança da Informação será revista e aprovada anualmente por parte do Comité de Cibersegurança do Grupo UCI. Não obstante, caso ocorram alterações relevantes na Sociedade ou sejam identificadas mudanças significativas no ambiente de ameaças e riscos, quer sejam de tipo operacional, legal, regulamentar ou contratual, proceder-se-á à sua revisão sempre que se considere necessário,assegurando assim que a Política permanece sempre adaptada à realidade da Sociedade.

As propostas de alteração ou adaptação serão aceites e validadas pelo Comité de Cibersegurança.

17.2 Gestão da Política de Segurança da Informação

A Política de Segurança do Grupo UCI, bem como todo o Corpo Normativo de Segurança relacionado (Normas e Procedimentos) estabelecem os requisitos mínimos de Segurança que todos os departamentos da Sociedade devem satisfazer nos seus contextos.

O Grupo UCI considera a Segurança da Informação como uma prioridade para a Organização e, por isso, a presente Política estabelece as seguintes orientações:

- A informação da qual o Grupo UCI é proprietário e/ou depositário apenas pode ser acedida pelas pessoas devidamente autorizadas, quer pertençam ou não à Sociedade.
- A presente Política e o seu desenvolvimento devem ser comunicados a todas as pessoas do Grupo UCI, tanto ao pessoal interno como, se for caso disso, ao pessoal externo do terceiro contratado, e estar sempre disponível às partes interessadas. No

caso do pessoal externo, realizar- se-ão as adaptações da Política que sejam aplicáveis em cada caso.

- O Grupo UCI deve cumprir todos os requisitos legais, regulamentares e estatuários que lhe sejam aplicáveis, bem como com os requisitos contratuais.
- A confidencialidade da informação deve ser sempre garantida.
- A integridade da informação deve ser assegurada através de todos os processos para a sua gestão ou processamento e armazenamento.
- A disponibilidade da informação deve ser garantida através das medidas adequadas de apoio e continuidade do negócio.
- Todo o pessoal com responsabilidades em matéria de Segurança da Informação deve dispor da adequada formação e consciencialização.
- Qualquer incidente ou fragilidade que possa comprometer ou tenha comprometido a confidencialidade, integridade e/ou disponibilidade da Informação deve ser registado e analisado para aplicar as respetivas medidas corretivas e/ou preventivas.

Para a prossecução dos objetivos desta Política, o Grupo UCI deve estabelecer uma estratégia preventiva de análise dos riscos que o possam afetar, identificando-os, implementando controlos para a sua mitigação e estabelecendo procedimentos regulares para a sua reavaliação. No decurso deste ciclo de melhoria contínua, o Grupo UCI deve manter a definição tanto do nível de risco residual aceite (apetência pelo risco) como dos seus limiares de tolerância.

17.3 Estrutura do Corpo Normativo de Segurança

O Corpo Normativo de Segurança deve seguir uma estrutura hierárquica de documentos definida em três níveis:

- Nível 1. Política de Segurança da Informação: trata-se do presente documento, que é o principal do Corpo Normativo de Segurança. Estabelece uma declaração de alto nível dos objetivos e do compromisso do Grupo UCI para a gestão da Segurança da Informação. Os restantes componentes do Corpo Normativo baseiam- se e desenvolvem-se a partir desta Política.
- Nível 2. Normas de Segurança da Informação: conjunto de documentos que suportam os objetivos reunidos na Política de Segurança do Grupo UCI. A este nível, indicam-se os requisitos de segurança com maior grau de detalhe para cada secção ou âmbito refletido na Política.
  Ainda que não estejam reunidos no Corpo Normativo de Segurança, é de assinalar a existência de documentos procedimentais, que reúnem o conjunto de tarefas detalhadas e especificadas com o intuito de apoiar a operação diária. Estas tarefas estão alinhadas com os requisitos de segurança estabelecidos nas Normas correspondentes. As Normas que desenvolvem a Política de Segurança da Informação estão enumeradas no documento *UCI.SGSI.NOR0000.Norma.Zero*.

As especificações e objetivos definidos na Política de Segurança, juntamente com os requisitos estabelecidos nas diferentes Normas de Segurança da Informação que constituem o Corpo

Normativo de Segurança do Grupo UCI são de cumprimento obrigatório por parte de todos os funcionários da Sociedade.

17.4 Aspetos Organizativos: Funções e Responsabilidades

A Segurança da Informação é conduzida a partir de um contexto de governo e gestão (ou seja, funções e responsabilidades, separação de funções, contacto com as autoridades e grupos de interesse especiais) e é estabelecida a necessidade de prever os requisitos de segurança no Grupo UCI para a gestão de projetos, a proteção interna e a externalização de serviços.

O Grupo UCI compromete-se a zelar pela Segurança de todos os ativos sob a sua responsabilidade através de medidas que sejam necessárias, garantindo sempre o cumprimento das diferentes Normas e leis aplicáveis.

Juntamos o *Anexo I*, onde se apresenta em detalhe a composição das equipas responsáveis pela definição, coordenação, manutenção e alteração das Políticas de Segurança do Grupo UCI. O *Anexo I* deve refletir as atualizações necessárias quando houver alterações do pessoal envolvido.

17.5 Gestão da Segurança dos Recursos Humanos

O Departamento de Recursos Humanos deve proceder à sua gestão, tendo em conta os critérios de segurança previstos na Política de Segurança, e esse departamento representa um ponto-chave para assegurar o cumprimento da mesma.

As responsabilidades em matéria de Segurança devem ser consideradas no processo de seleção de pessoal, na elaboração dos contratos e durante a fase laboral, a fim de reduzir os riscos de manipulação, roubo, fraude ou utilização inadequada da Informação.

As obrigações contratuais para os funcionários devem refletir-se nas Políticas e Normas de Segurança do Grupo UCI. Os termos e condições devem incluir aspetos como acordos de confidencialidade, direitos legais, responsabilidades pelo cumprimento do Corpo Normativo e pelo tratamento de Informação de terceiros e ações a tomar se a pessoa não cumprir os requisitos de Segurança.

Todo o pessoal da Sociedade recebe um nível de formação e consciencialização em matéria de Segurança da Informação. Por outro lado, cabe aos funcionários operar com diligência em relação à informação, devendo-se assegurar que essa informação não fique na posse de terceiros não autorizados. Do mesmo modo, devem ser informados sobre as atualizações das Políticas e Normas de segurança que lhes digam respeito e das ameaças existentes, de forma que o cumprimento desta Política seja garantido.

17.6 Gestão de Ativos

O Grupo UCI estabelece um conjunto de medidas para organizar os ativos de informação, manter a sua integridade e protegê-los de fugas, apagamentos acidentais ou acessos não autorizados.

Toda a informação da Sociedade é classificada para facilitar os processos de controlo de acesso, guarda e monitorização. Com base no nível de classificação da informação estabelecido, o Grupo UCI estabelece medidas e controlos preventivos, e quanto mais confidencial for considerada a

informação, mais restritivos são esses controlos.

O Grupo UCI também estabelece as orientações de utilização e manipulação de dispositivos móveis (portáteis, telemóveis, smartphones, tablets, etc.), entre outros, fornecidos pela Sociedade e pessoais que utilizem os seus sistemas de informação.

Ao mesmo tempo, proíbe-se o armazenamento de informação proprietária do Grupo UCI em sistemas não corporativos e o uso de dispositivos pessoais fica restringido e deve ser analisado para avaliar o risco que poderia trazer à Sociedade. Em caso de aceitação, esta será registada como exceção e deve ser feito um seguimento da mesma.

Por outro lado, o emprego e boa utilização de tecnologias críticas (correio eletrónico, Internet, redes sociais) está definido de forma a manter uma elevada segurança e mitigar qualquer risco que possa vir a ser provocado devido a um mau uso destas tecnologias.

17.7 Controlo de Acesso

O acesso por parte do pessoal interno ou externo aos sistemas ou instalações do Grupo UCI, bem como à informação ou ativos que sejam utilizados, é regulado com base nas necessidades de informação e operação de cada utilizador, concedendo acesso exclusivamente às funções e informação que sejam necessárias para o correto desempenho da sua atividade laboral.

Os responsáveis pelos ativos são responsáveis por definir os níveis de acesso aos recursos e autorizar qualquer acesso extraordinário, bem como por rever regularmente os direitos de acesso dos utilizadores.

Todos os acessos efetuados aos Sistemas de Informação do Grupo UCI ficam associados a um processo de identificação, autenticação e autorização, estabelecendo-se os controlos necessários para que esses processos sejam efetuados de forma segura.

Existem mecanismos de registo, monitorização de acesso e uso dos sistemas, que permitam conhecer a eficácia das medidas implementadas e detetar possíveis incidentes de Segurança.

De forma a garantir estas medidas de segurança, os utilizadores devem ser únicos e não podem ser partilhados, salvo exceções devidamente autorizadas, avaliadas e documentadas. Todos eles são inicialmente atribuídos mediante o Princípio do Privilégio Mínimo.

O acesso às instalações onde se realizem processos críticos para o Grupo UCI tem um controlo adequado para minimizar o impacto na continuidade das operações dos processos comerciais, reduzindo o tempo de indisponibilidade aos níveis estabelecidos.

17.8 Controlos Criptográficos

O Grupo UCI aplica controlos criptográficos com base na necessidade de implementar esses controlos em função do nível de Segurança exigido pela

tipologia de Informação existente nos diferentes contextos e plataformas para garantir a confidencialidade da informação.

As medidas criptográficas estão alinhadas com o esquema de classificação de dados do Grupo UCI e são implementados mecanismos e ferramentas de encriptação que sejam imunes aos

ataques criptográficos mais comuns.

O Grupo UCI implementa controlos criptográficos em meios removíveis que contenham informação considerada como crítica, de acordo com o esquema de classificação da Sociedade, como é o caso de discos rígidos, portáteis, móveis, servidores e bases de dados.

As chaves de encriptação são armazenadas nos sistemas corporativos destinados a esse fim, ser adequadamente protegidas e o acesso às mesmas apenas deve ser permitido através de um processo rigoroso de autorização, com o intuito de preservar a sua confidencialidade. Do mesmo modo, é definido o período de vida das chaves de encriptação no momento da sua criação.

17.9 Segurança Física e do Ambiente

Os espaços físicos onde estão situados os sistemas de Informação, bem como os destinados ao âmbito laboral do Grupo UCI, estão adequadamente protegidos. O Grupo UCI também estabelece medidas de Segurança para proteger os ativos físicos dentro e fora do contexto laboral.

17.10 Informação em Suporte Digital ou Informático

A presente Política aplica-se também à informação proprietária do Grupo UCI que esteja em formatos diferentes do digital ou informático, como é o caso das cópias impressas, as notas realizadas manualmente, as anotações realizadas em quadros que estejam expostos à vista, etc.

Neste sentido, o Grupo UCI toma as medidas de segurança necessárias para proteger estas fontes de informação.

17.11 Segurança na Operação

Todos os sistemas de Informação do Grupo UCI dispõem das medidas de segurança que otimizem o nível de maturidade dos sistemas que são processados ou armazenados na Empresa. Do mesmo modo, as redes devem ser geridas e controladas de forma adequada, a fim de serem protegidas de ameaças e manter a segurança dos sistemas e aplicações que utilizem a rede, incluindo os controlos de acesso, protegendo assim toda a Informação que seja transferida através destes elementos e/ou contextos.

São formalmente estabelecidas responsabilidades e Procedimentos documentados para assegurar uma correta configuração, administração, operação e monitorização dos Sistemas de Informação do Grupo UCI. Para isso, deve seguir-se a respetiva Norma e adotar-se as melhores práticas em matéria de segurança.

São definidas, planeadas e realizadas auditorias periódicas aos Sistemas de Informação do Grupo UCI, com o objetivo de verificar o grau de cumprimento das diferentes Normas e a eficácia dos controlos aplicados para esse fim.

Essas auditorias, dependendo da criticidade do ativo de informação em causa, podem incluir atividades próprias de *hacking* ético, deteção de vulnerabilidades, testes de penetração ou técnicas semelhantes.

17.12 Segurança no Trabalho na Nuvem

A utilização uso cada vez mais intensiva pelo Grupo UCI de modelos de trabalho na Nuvem ou *Cloud Computing* implica riscos concretos para a Segurança da Informação, que é necessário controlar de forma específica. Para esse efeito, o Grupo UCI mantém uma Norma de Segurança na Nuvem que estabelece as medidas de segurança adequadas para garantir a confidencialidade, integridade e disponibilidade da sua informação, tendo em conta que a responsabilidade sobre a informação e os ativos continua a recair sobre a Sociedade.

17.13 Segurança nas Telecomunicações

A Informação transmitida por redes de comunicações, públicas ou privadas, está adequadamente protegida por meio de mecanismos de segurança que garantam a sua confidencialidade, disponibilidade e integridade. São estabelecidos os controlos necessários que impeçam golpes de *phishing* por parte do emissor, alteração ou perda da Informação transmitida, tanto nas comunicações com sistemas localizados nas redes internas, como com entidades com as quais o Grupo UCI tenha relação.

As arquiteturas de redes do Grupo UCI dispõem de medidas de prevenção, deteção e resposta para evitar violações nos domínios internos e externos, sendo da máxima importância a administração de segurança das redes que atravessam o perímetro do Grupo UCI, implementando controlos adicionais para os dados sensíveis que circulem pelas redes de comunicação públicas.

Sempre que seja tecnologicamente possível, deve realizar-se uma segregação entre as redes de dados e rede de segurança, de forma a preservar a integridade da informação que nelas circula.

Quanto à ligação remota às redes do Grupo UCI, estabelece-se um conjunto de tecnologias e controlos de segurança de acordo com o perfil de utilizador.

Os riscos associados às redes sem fios terão o mesmo tratamento que os riscos referentes às redes por cabo, tendo em conta as particularidades de ambos os tipos de redes.

17.14 Segurança no Ciclo de Vida dos Sistemas

Os requisitos de segurança devem ser considerados durante todo o Ciclo de Vida de Desenvolvimentos e das Infraestruturas Tecnológicas do Grupo UCI, tanto nos sistemas de desenvolvimento próprio como nos desenvolvidos por terceiros, desde as fases de análise de requisitos e viabilidade, em que esses requisitos são detalhados e avaliados, até às fases de conceção, testes, implementação, aceitação e sua posterior manutenção.

Para o correto desenvolvimento de software, deve existir um plano de testes de segurança que inclua revisões de código seguro, proteção de dados, etc. Também serão realizados testes de penetração e análise de vulnerabilidades sobre qualquer desenvolvimento de software antes da sua produção.

Cada unidade de negócio do Grupo UCI deve ter em conta a Segurança da Informação nos seus processos e procedimentos de seleção, desenvolvimento e implementação de aplicações, produtos e serviços.

O Grupo UCI realiza comunicações aos programadores de sistemas sobre as Normas de segurança e os seus objetivos, bem como outras Normativas aplicáveis.

17.15 Segurança nos Fornecedores

O Grupo UCI presta especial atenção à avaliação da criticidade de todos os serviços suscetíveis de ser subcontratados, de forma a poder identificar os que sejam relevantes do ponto de vista da Segurança da Informação, seja pela sua natureza, pela sensibilidade dos dados que devam ser tratados ou pela dependência sobre a continuidade do negócio.

Relativamente aos prestadores destes serviços, são cuidadosamente geridos os processos de seleção, os requisitos contratuais, a monitorização dos níveis de serviço e as medidas de segurança implementadas por esses prestadores. É obrigatória a apresentação de evidências sobre o bom estado do prestador tanto em matéria de segurança como de conformidade com a legislação fiscal e laboral, sendo esta verificação realizada periodicamente com base na categorização do risco de cada prestador.

Score riesgo	Plazo/años
Bajo / Medio-Bajo	3
Medio-alto	2
Alto	1
Externalizaciones esenciales	1

Dispomos de processos formais para a celebração da relação com os fornecedores, que incluam cláusulas contratuais específicas para assegurar a privacidade e a devolução ou eliminação da Informação uma vez terminado o serviço.

17.16 Gestão de Ciberincidentes

Todos os funcionários do Grupo UCI têm a obrigação e responsabilidade de identificar e notificar o responsável pela Cibersegurança da Sociedade acerca de qualquer incidente ou delito que possa comprometer a segurança dos seus ativos de informação.

O Grupo UCI também implementou Procedimentos para a correta gestão dos incidentes detetados.

O Grupo UCI dispõe de um processo de resposta perante incidentes para gerir de forma correta todas as ameaças materializadas na Organização. Este processo inclui aspetos como a monitorização, acompanhamento, classificação e correção desses incidentes.

Qualquer incidente que possa comprometer ou tenha comprometido a confidencialidade, integridade e/ou disponibilidade da Informação deve ser registado e analisado para aplicar as respetivas medidas corretivas e/ou preventivas.

Foi estabelecido um plano de simulações que apoiem a formação e sensibilização do pessoal da Empresa.

17.17 Continuidade do Negócio

Respondendo a requisitos de qualidade e boas práticas, o Grupo UCI dispõe de um Plano de Continuidade do Negócio como parte da sua estratégia para garantir a continuidade na prestação dos seus serviços essenciais e a adequada gestão dos impactos sobre o negócio perante possíveis cenários de crise, proporcionando um quadro de referência para que a Sociedade atue caso seja necessário. Este Plano de Continuidade deve ser revisto e testado periodicamente.

No desenvolvimento deste plano, deve ser considerado não apenas o plano de contingência dos Sistemas de Informação, como também dos próprios Serviços de Segurança, as dependências físicas, as pessoas que prestam apoio à atividade comercial e os recursos que possam ser necessários para que a Organização possa continuar a desenvolver a sua atividade produtiva e de atendimento aos clientes.

O plano de contingência desenvolve e implementa para assegurar que os processos críticos do negócio possam ser restabelecidos no tempo exigido, incluindo controlos para identificar e reduzir os riscos, limitando as consequências dos incidentes que afetem negativamente, e assegurando o tempo de resposta das operações essenciais.

Dentro deste plano, são partes fundamentais a formação aos membros da equipa de gestão de crises, bem como o exercício de testes e verificação regular sobre os planos de resposta definidos.

O plano deve ser revisto e publicado, pelo menos, uma vez por ano ou quando, por causas suficientes, sofra alterações importantes, como novos ativos imobiliários, tecnológicos, organizacionais.

Qualquer Informação sensível, confidencial ou dados de caráter pessoal deve ser registada em cópias de back-up. A gestão destas cópias de Segurança deve ser efetuada e conservada de acordo com as medidas de Segurança definidas pelo Grupo UCI.

17.18 Cumprimento Normativo Legal

O Grupo UCI compromete-se a dotar dos recursos necessários para dar cumprimento a toda a legislação e regulamentação aplicável à atividade da Sociedade em matéria de Segurança da Informação, e estabelece que a responsabilidade por esse cumprimento recai sobre todos os seus membros. Neste sentido, deve assegurar-se o cumprimento de toda a legislação, Normativa ou regulamentação aplicável.

Com o objetivo de assegurar a confidencialidade, a integridade e disponibilidade da informação, e detetar possíveis incumprimentos, os sistemas do Grupo UCI estarão sujeitos à realização periódica de atividades de auditoria e monitorização.

17.19 Gestão de Exceções

Qualquer exceção ao Corpo Normativo de Segurança deve ser registada e informada ao Comité de Cibersegurança do Grupo UCI, bem como aprovada pelo mesmo. Estas exceções serão analisadas para avaliar o risco que poderiam introduzir à Sociedade e, com base na categorização destes riscos, eles devem ser assumidos pelo requerente da exceção, juntamente com os responsáveis pelo negócio. Deve ser feito um acompanhamento dessas exceções.

17.20 Sanções Disciplinares

Qualquer violação da presente Política de Segurança pode resultar na tomada de ações disciplinares correspondentes, de acordo com o Procedimento Disciplinar do Grupo UCI. Todos os membros do Grupo UCI têm a responsabilidade de notificar o responsável pela Cibersegurança acerca de qualquer evento ou situação que possa implicar o incumprimento de alguma das orientações definidas pela presente Política, conforme previsto no parágrafo 8.16 Gestão de Ciberincidentes deste documento.

18. Anexos

18.1 Responsáveis pela Coordenação da Política de Segurança

Equipa/Função	Responsabilidades
Comité de Cibersegurança	Aprovação e coordenação. Coordena a Segurança da Informação na Sociedade. Será composto por membros do Comité de Direção, pelo Responsável pela Cibersegurança e por representantes de outras áreas do Grupo UCI.
CISO	Responsável pela Segurança da Informação. Este cargo é ocupado pelo CISO do Grupo UCI: David Espantaleón
Responsável pela Cibersegurança	Responsável pela Segurança operacional
Responsável pelo Serviço	Responsável por estabelecer os requisitos de um serviço em matéria de segurança.
Utilizadores	Aplicar e cumprir.

Nota: Esta informação deve ser atualizada quando existam alterações dos membros das equipas responsáveis pela coordenação. Os requisitos indicados são desenvolvidos no Procedimento de Modelo de Governo de Segurança.