Política de Seguridad de la Información

Tabla de contenido

Nivel:	Corporativo	Creado por:	Víctor Pena
Propietario:	IT Manager	Aprobado por:	Germán Serna
Plantas afectadas:	Grupo Cosmos XXI y Sociedades	Fecha:	07/05/2021

Versiones	Fecha	Modif.
1	20/011/2020	Creado
2	07/05/2021	Modificado

Política de Seguridad de la Información

1. OBJETO

Establecer los objetivos de la política de seguridad de la información para Grupo Cosmos y sus sociedades.

2. OBJETIVO

El Consejo de Administración ha aprobado en su sesión de 26 de enero de 2021, previo informe favorable de la Comisión de Auditoría y Cumplimiento y a propuesta del Comité de Seguridad de la Información (en adelante, también el "**CSI**"), la presente Política de Seguridad de la Información (en adelante, también la "**Política**"), que establece los principios y directrices con los que Grupo Cosmos XXI (en adelante, también la "**Grupo**" o la "**Sociedad**") protegerá su información, de conformidad con la normativa aplicable y con sus valores éticos, definidos en el Código de Conducta y Prácticas Responsables (en adelante, el "**Código de Conducta**") así como con lo previsto en el Reglamento del Comité de Seguridad de la Información (en adelante, el "**Reglamento**") y en otra normativa interna que resulte de aplicación.

Grupo Cosmos XXI velará por la protección de la información, independientemente de la forma en la que esta se comunique, comparta, proyecte o almacene (en adelante, la "**Información**"). Esta protección afecta tanto a la información existente dentro del Grupo como a la información compartida con terceros.

En este sentido, se entiende por Seguridad de la Información, la salvaguarda y protección de (i) la Información titularidad de Grupo Cosmos XXI, con independencia de que se encuentre en sistemas propios o de terceros; y (ii) la información titularidad de terceros, que se encuentre en sistemas de Grupo Cosmos XXI.

A los efectos de la presente Política, se entiende por Sistemas de Información el conjunto de tecnologías o medios tecnológicos, propios o de terceros que gestionen, almacenen o transmitan Información (incluyendo tecnologías en la nube o similares).

3. ALCANCE

La presente Política se aplicará a la Sociedad y a su Grupo de empresas, y vinculará a todo su personal, independientemente de la posición y función que desempeñe.

A estos efectos, se entiende por Grupo las sociedades en las que Grupo Cosmos XXI S.L sea participe en el accionariado o gestión de las mismas tanto vertical como horizontalmente.

La aplicación de la Política podrá hacerse extensiva, total o parcialmente, a cualquier otra persona física y/o jurídica vinculada con el Grupo por una relación distinta de la laboral cuando ello sea posible por la naturaleza de la relación y resulte conveniente para el cumplimiento de la finalidad de aquella.

De conformidad con la Política, Grupo Cosmos XXI podrá desarrollar procedimientos e instrucciones para implementar y dar cumplimiento a las obligaciones asumidas, así como para adaptar la misma a las diversas legislaciones locales aplicables al Grupo.

Asimismo, la aplicación de esta Política es complementaria a otras normas internas de obligado cumplimiento, como la Política de Cumplimiento en Materia de Protección de Datos Personales y Privacidad, y aquellas otras que regulen cuestiones relacionadas con la información de la Compañía.

4. PRINCIPIOS GENERALES

La consecución de los objetivos descritos en el apartado 3 se articula a través de los siguientes principios generales:

-Clasificación de la Información. La Información se clasificará en función a su valor, importancia y criticidad para el negocio, de forma que las medidas de protección se adecúen al nivel de clasificación de cada activo de información. Del mismo modo, la clasificación de los activos de Información se realizará tomando en consideración los requisitos legales, operacionales y las buenas prácticas y estándares al respecto.

-Uso de los Sistemas de Información. El uso de los Sistemas estará limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.

-Segregación de funciones. Se deberán evitar las concentraciones de riesgos derivados de la ausencia de segregación de funciones y la dependencia unipersonal de funciones críticas para el negocio.

En este sentido, se deberán establecer procedimientos formales para controlar la asignación de privilegios a los Sistemas de Información, de forma que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

-Retención de la Información. Se establecerán, cuando resulte necesario o conveniente, períodos de retención de la Información por categorías atendiendo a las necesidades operativas o de cumplimiento regulatorio, así como los correspondientes procedimientos de destrucción de la Información.

-Acceso a la Información por parte de terceros. Se desarrollarán los procedimientos de control de la puesta a disposición y acceso por terceros a la Información relativa a Grupo Cosmos XXI o de cualesquiera otros terceros relacionados con el Grupo.

-Seguridad de la Información en los Sistemas. Los entornos de desarrollo y producción se mantendrán en Sistemas independientes. Igualmente, el desarrollo y mantenimiento de los Sistemas de Información deben incluir los controles y registros necesarios para garantizar la correcta implementación de las especificaciones de seguridad.

-Continuidad. Se establecerá un proceso de gestión de continuidad que permita garantizar la recuperación de la Información crítica para el Grupo en caso de desastre, reduciendo el tiempo de indisponibilidad a niveles aceptables.

-Cumplimiento. Los Sistemas de Información y comunicaciones del Grupo deberán estar adecuados de forma permanente a las exigencias de la legislación vigente en todas las jurisdicciones en las que opera, así como a la normativa interna de desarrollo que resulte de aplicación.

La responsabilidad de la protección de la Información y de los Sistemas que la tratan, almacenan o transmiten se extiende a todos los niveles organizativos y funcionales de Grupo Cosmos XXI, cada uno en la medida que le corresponda, como se detalla a continuación:

5. RESPONSABILIDADES DE LOS EMPLEADOS

- Todos los empleados del Grupo deberán conocer, asumir y cumplir la Política, así como la normativa interna de seguridad y uso de los Sistemas vigentes, estando obligados a mantener el secreto profesional y la confidencialidad de la Información manejada en su entorno laboral y debiendo comunicar, con carácter de urgencia y según los procedimientos establecidos, las posibles incidencias o problemas de seguridad que se detecten.

- Los empleados que contraten servicios de terceros que impliquen el uso o acceso de estos últimos a la Información deberán entender los riesgos derivados del proceso de externalización y asegurar una gestión eficaz de los mismos.
- El uso de los Sistemas o servicios digitales por parte de los empleados, incluyendo expresamente el correo electrónico y los servicios de mensajería instantánea, estará limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.

5.1 Responsabilidades en relación con proveedores y otros terceros

- De forma complementaria al apartado 5.1, los contratos con terceros que impliquen el uso o acceso de estos últimos a la Información, entre los que se encuentran los de prestación de servicios o contratos de externalización, incluirán requerimientos específicos de seguridad relativos a la tecnología y las actividades de aquellos que llevan a cabo dichos servicios.

  • En este sentido, deberán incluir provisiones mediante las que se garantice que los proveedores, el personal subcontratado o cualquier empresa externa que utilice o acceda, de manera potencial o real, a la Información (a través de los Sistemas o de cualquier otro medio, como se expone en el apartado 1), deberán conocer y cumplir la Política en lo que les sea de aplicación, estando obligados a mantener el secreto profesional y la confidencialidad de la Información manejada en su relación con el Grupo.

5.2 Departamento de Seguridad de la Información

El Departamento de Seguridad de la Información ejercitará su función de control de manera independiente y es su responsabilidad implementar esta Política y monitorizar su cumplimiento, así como el de todos los requerimientos derivados de las leyes, normas y buenas prácticas en materia de seguridad de la Información que sean de aplicación. Por ello, es responsable de:

- Implementar una estrategia de seguridad de la Información que vele por el cumplimiento de los principios básicos de esta Política, y en particular que dé cobertura a los siguientes aspectos:
  - un adecuado acceso a la Información, basado en el principio de mínimo privilegio y la aprobación del dueño del activo de Información;
  - una segregación adecuada de roles y funciones en los Sistemas de Información; o una correcta configuración, administración y operación de la infraestructura, servicios y/o del *software* utilizado en los distintos procesos de negocio tanto dentro, como fuera de las instalaciones del Grupo, desde el punto de vista de la seguridad;
  - una correcta implementación de los requisitos de seguridad durante el ciclo de vida de los Sistemas de Información que dan soporte a los procesos de la Compañía.
  - una adecuada protección de los Sistemas y la Información que soportan frente a amenazas físicas o ambientales, en atención a su criticidad, que permita identificar, evaluar, prevenir y responder a cualquier riesgo que pueda comprometer su seguridad.
- Establecer y revisar los controles correspondientes para asegurar el cumplimiento de esta Política y su normativa de desarrollo, incluyendo los mecanismos organizativos y tecnológicos necesarios para facilitar la monitorización continua de las actividades del acceso y uso de los Sistemas, servicios o Información gestionados por el Grupo.

- Prevenir, detectar y responder ante cualquier incidente en materia de Seguridad de la Información y actuar de acuerdo con lo establecido en el "Procedimiento Relativo a la Seguridad de la Información: Plan de Respuesta ante Incidentes del Grupo Grupo Cosmos XXI".
- Impulsar el desarrollo normativo de la presente Política, mediante los procedimientos o instrucciones que sean necesarios para definir un marco global de actuación de la seguridad de la Información en todos sus ámbitos. Igualmente, deberá revisar, actualizar y comunicar cualquier cambio que derive en variaciones de esta Política.
- Realizar actividades de formación y concienciación en materia de los procesos de Seguridad de la Información.
- Establecer un enfoque de mejora continua.
- Velar por el cumplimiento con la legislación vigente en el ámbito de las competencias que le atribuye la presente Política.

5.3 Comité de Seguridad de la Información

Grupo Cosmos XXI cuenta con un Comité de Seguridad de la Información integrado por miembros de la Dirección que, en cumplimiento del Reglamento, tiene por objetivo asegurar que las buenas prácticas sobre la gestión de la seguridad se apliquen de manera efectiva y consistente en todo el Grupo.
Entre otras funciones, asume la responsabilidad de supervisar la estrategia de seguridad de la Información, incluyendo los planes de gasto, inversión y recursos en seguridad, y coordinar las necesidades de seguridad de la dirección, de los negocios y de las geografías.
También deberá informar a través del Departamento de Seguridad de la Información, al menos anualmente, al Presidente Ejecutivo y a los Órganos de Gobierno de Grupo Cosmos XXI que corresponda, sobre el estado de la seguridad, la evolución de las amenazas y el apetito de riesgo, la asignación de los recursos destinados a la seguridad y sobre los incidentes significativos.

6. IMPLEMENTACION Y FUTUROS PROYECTOS

Grupo Cosmos XXI se compromete a asignar recursos específicos para asegurar la implementación efectiva de la Política.
Grupo Cosmos XXI se compromete a tener en cuenta los requisitos de seguridad de la información para futuros proyectos con ánimo de garantizar la seguridad y cumplimiento sobre los sistemas de información.

7. CONTROL Y AUDITORIA

Grupo Cosmos XXI se reserva expresamente el derecho de adoptar, con proporcionalidad, las medidas de vigilancia y control necesarias para comprobar la correcta utilización de los sistemas que pone a disposición de sus empleados, incluyendo el contenido de las comunicaciones y dispositivos, respetando, en todo caso, la legislación vigente y garantizando la dignidad del empleado. La comunicación y aceptación de esta Política será válida a efectos de notificación previa al trabajador.

El Grupo se someterá a revisiones y controles periódicos, así como auditorías internas y externas para evaluar el cumplimiento general de esta Política.

La valoración de un posible incumplimiento de esta Política se determinará en el procedimiento correspondiente, según las disposiciones vigentes, sin perjuicio de las responsabilidades legales, incluso de carácter sancionador en el ámbito laboral, que, en su caso, puedan resultar exigibles al incumplidor.

8. COMUNICACIÓN DE LA POLÍTICA

La presente Política estará disponible en la intranet de Sharepoint Online de Grupo Cosmos XXI para todos los empleados y estará disponible para todos los grupos de interés de la Compañía en la web corporativa (www.gcosmos.com). Asimismo, la Política será objeto de las adecuadas acciones de comunicación, formación y sensibilización para su oportuna comprensión y puesta en práctica.

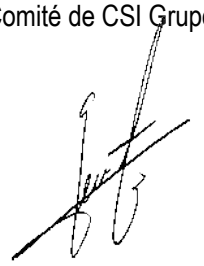
9. ACTUALIZACION DE LA POLÍTICA

La Política será revisada y actualizada cuando proceda, con el fin de adaptarla a los cambios que puedan surgir en el modelo de negocio o en el contexto donde opere Grupo Cosmos XXI, garantizando en todo momento su efectiva implantación.

Repr. Consejo Administración Grupo Cosmos XXI S.L

Firmado

Comité de CSI Grupo Cosmos XXI S.L



Firmado