# Política Corporativa de Seguridad de la Información

Consejero Delegado
28 abril 2023

**CONTROL DE VERSIONES**

| Versión | Fecha | Cambios |
|---|---|---|
| V1 | 31/07/2020 | Nueva Creación |
| V2 | 28/04/2023 | Adaptación a ISO/IEC 27001:2013 |

# CONTENIDO

# 1. Objeto

La Política Corporativa de Seguridad de la Información tiene por objeto establecer y regular las disposiciones generales y los principios rectores de las cuestiones de seguridad de la información que conciernen a la Compañía.

URBASER, se reafirma en su posición como Compañía orientada a la sostenibilidad a través de su misión de contribuir al adecuado desarrollo de ciudades y territorios mediante servicios eficientes y tecnología innovadora. Por ello, desempeña un papel relevante en la protección de la actividad tecnológica, industrial y comercial en el desarrollo y operación de las infraestructuras críticas que prestan servicios esenciales a la sociedad y a las entidades e instituciones públicas gubernamentales.

URBASER debe estar perfectamente preparada para intervenir, reaccionar y proteger sus activos de información ante incidentes de seguridad que puedan afectarle, así como para que la totalidad de sus actividades y servicios se encuentren alineados con las más exigentes directrices locales e internacionales de seguridad de la información.

Mediante la aprobación de esta Política, URBASER manifiesta su determinación y compromiso en alcanzar un nivel de seguridad de la información adecuado a las necesidades del negocio que garantice la protección de los activos de forma homogénea en todo el Grupo.

# 2. Ámbito de Aplicación

Esta Política es de aplicación en la totalidad de las entidades participadas (sociedades, UTEs, Joint Ventures o cualquier otra fórmula asociativa) en las que URBASER, S.A.U. sea el socio mayoritario o tenga el control (en adelante, "URBASER") y de obligado cumplimiento a todo usuario que participe en la gestión, uso o explotación de la Información de URBASER, incluido, pero no limitado a consejeros/as, directivos/as, empleados/as, colaboradores, gerentes, miembros de los órganos de gobiernos.

En aquellas entidades participadas en las que esta Política no sea de aplicación, se promoverá, a través de sus representantes en los órganos de administración, el alineamiento de sus políticas propias con las de la presente Política.

# 3. Contenido

La seguridad de la información, uno de los pilares fundamentales sobre los que se construye URBASER, ha de entenderse como un concepto integral que tiene por finalidad preservar los activos y proteger los intereses y objetivos estratégicos de la Compañía. De igual forma, la seguridad de la información ha de contribuir a preservar la confidencialidad, integridad y disponibilidad de los datos de los clientes y otras partes interesadas.

En este sentido, URBASER, asume los siguientes objetivos:

- Alinear la estrategia de seguridad de la información con la estrategia de negocio de URBASER.
- Establecer un buen gobierno de seguridad de la información para asegurar su correcta gestión y operación conforme a los requisitos aplicables en la materia (la legislación aplicable vigente en cada país, los requisitos contractuales y necesidades de las partes interesadas).
- Aportar los recursos que sean necesarios para alcanzar los objetivos establecidos.
- Identificar y, cuando proceda, evaluar y categorizar los riesgos y oportunidades inherentes a las actividades, procesos y servicios, planificando las acciones necesarias para su tratamiento, previniendo los efectos no deseados y

potenciando los efectos favorables de los mismos.

- Asegurar la cadena de suministro desde el punto de vista de seguridad de la información.
- Asegurar que todo el personal, incluyendo los colaboradores externos con acceso a los sistemas de información de la organización, cuenta con la cultura, formación, concienciación y capacitación adecuada para el desarrollo de sus actividades de forma segura para sí mismos y para los demás, garantizando en todo momento la seguridad de la información.
- Implantar las medidas de seguridad necesarias para velar por la confidencialidad, integridad y disponibilidad de la seguridad de la información en todo su ciclo de vida.
- Gestionar los incidentes de seguridad de la información para minimizar el impacto y la probabilidad de materialización de estos.
- Alinear la estrategia de gestión la seguridad de la información con la estrategia de continuidad de negocio IT.
- Mejorar de forma continua el sistema de gestión de la seguridad de la información, fomentando la participación activa de toda la organización para promover y adoptar medidas que conformen procesos más seguros y optimizados.

Con el fin de que las amenazas existentes en URBASER no se materialicen o, en caso de materializarse, no afecten gravemente ni a la información que maneja ni a los servicios prestados, las actividades de seguridad de URBASER se guiarán por los siguientes principios:

- **Eficiencia:** se priorizará el conocimiento de las potenciales amenazas y los riesgos derivados de las mismas, con el objetivo de adelantarse a su acción, evolución y para preservar a la Compañía de sus potenciales efectos dañinos, mitigándolos hasta un nivel aceptable para el negocio.
- **Responsabilidad:** los usuarios deben preservar la seguridad de los activos que URBASER pone a su disposición, en consonancia con los criterios, requisitos, procedimientos y tecnologías de seguridad definidos.
- **Legalidad:** se observará en todo momento el necesario cumplimiento de las leyes y regulaciones en materia de seguridad, vigentes en cada momento en todos los territorios en los que opera URBASER.
- **Cooperación y Coordinación:** se priorizarán la cooperación y la coordinación entre todas las unidades de negocio y plantilla, para generar las sinergias adecuadas y reforzar las capacidades conjuntas.
- **Prevención:** para prevenir y evitar que la información o los servicios se vean perjudicados por incidentes de seguridad, URBASER implementará las medidas de seguridad determinadas por la normativa de seguridad vigente en la actualidad en cada país, así como cualquier otro control adicional identificado a través de una evaluación de amenazas y riesgos.
- **Detección:** se monitorizará la operación de los sistemas y servicios de manera continua para detectar anomalías en los niveles de prestación y actuar en consecuencia.
- **Respuesta:** se establecerán mecanismos para responder eficazmente a los incidentes de seguridad de la información.
- **Recuperación:** se desarrollarán planes de continuidad de los sistemas de Tecnologías de la Información y la Comunicación (TIC).

Con el fin de dar cumplimiento a la presente norma, los roles y responsabilidades en materia de seguridad de la información están definidos en la Normativa de Roles y Responsabilidades (NS-19-CORP), donde está definido el Comité de Seguridad de la Información, órgano director de la presente Política.

# 4. Formación

Se promoverán las acciones de formación y concienciación necesarias para el conocimiento, implantación y seguimiento de la presente Política en materia de seguridad de la información.

# 5. Dudas, comunicaciones o denuncias

Las consultas en el ámbito de esta Política deben ser dirigidas al Área Corporativa de Seguridad de la Información de URBASER.

Cualquier incidencia en relación con el incumplimiento de lo establecido en esta Política y procedimientos relacionados, o su alineamiento con lo establecido en el Código de Conducta del Grupo, deberá dirigirse al órgano de cumplimiento normativo correspondiente a través del Canal Ético habilitado en la página web del Grupo (https://www.urbaser.com/canal-etico/).

# 6. Incumplimientos

La presente Política tiene la consideración de una norma de obligado cumplimiento, por lo que su vulneración supondrá una infracción de esta y la Compañía adoptará las medidas disciplinarias, contractuales o legales que sean procedentes, en su caso, sin perjuicio de otras responsabilidades en que el infractor hubiera podido incurrir. Igualmente, URBASER se reservará el derecho de adoptar las medidas que considere oportunas contra los socios comerciales que la incumplan.

# 7. Revisión y actualización

El Comité de Seguridad de la Información revisará anualmente o siempre y cuando exista un cambio sustancial en el contexto de la organización, asegurándose de que recoge las recomendaciones y mejores prácticas internacionales acorde con los requisitos normativos y legislación aplicable. También propondrá al Órgano de Administración las modificaciones y actualizaciones que contribuyan a su desarrollo y mejora continua.

www.urbaser.com