MEDIDAS DE CIBERSEGURIDAD PARA PROVEEDORES

INFORMACIÓN GENERAL

INTRODUCCIÓN:

Con el fin de asegurar el cumplimiento de las normativas y regulaciones vigentes e internas, así como mantener un nivel adecuado de seguridad de la información y procesos industriales del Grupo Urbaser (en adelante, la Compañía), **se informa a los proveedores que deben aplicar obligatoriamente una serie de medidas de seguridad que protejan los recursos y sistemas frente a amenazas, asegurando la disponibilidad, integridad y confidencialidad.**

ALCANCE:

En términos generales, proveedores que **suministren productos, servicios y/o soluciones relacionadas con la tecnología** (informática, electrónica, o cualquier otro aspecto que facilite la operación, gestión o mejora de sistemas), **o que accedan a sistemas IT y/u OT, así como a procesos industriales de la Compañía y/o traten información o datos personales de la Compañía.**

A continuación, se presentan de manera general algunas medidas básicas y relevantes que los proveedores deben cumplir, basadas en estándares internacionales y buenas prácticas. Estas medidas se reflejarán con más detalle en la documentación contractual.

RESUMEN MEDIDAS DE CIBERSEGURIDAD

- **Aspectos generales:** El Proveedor deberá implementar medidas técnicas, organizativas y legales para garantizar la seguridad de la información, los procesos y datos personales de la Compañía, evitando su alteración, pérdida, tratamiento o acceso no autorizado, considerando la tecnología, la naturaleza de los datos tratados y los riesgos a los que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

  Para ello, el Proveedor deberá demostrar la implementación de buenas prácticas de seguridad, preferiblemente mediante certificaciones que acrediten la adopción y uso de un sistema de gestión de la seguridad de la información, por ejemplo, ISO/IEC 27001, ENS, NIS 2, ISO/IEC 62443, etc.

- **Confidencialidad:** Toda la información proporcionada por la Compañía es confidencial y debe usarse únicamente para el cumplimiento del objeto del contrato y no debe compartirse sin autorización previa de la Compañía.

- **Gestión de la seguridad de la información:** Notificar cualquier cambio que afecte la seguridad de la información, capacitar a los usuarios en seguridad y privacidad y permitir auditorías de sus sistemas. Así mismo, el Proveedor debe contar con mínimos como mantener dispositivos actualizados, con licencias vigentes y contar con conexiones seguras.

- **Gestión de incidentes y brechas de seguridad:** Disponer de un proceso definido de gestión de brechas e incidentes de seguridad, detallando aspectos de notificación, gestión y evaluación de estos. Especialmente, el Proveedor reportará cualquier incidente o brecha que pueda afectar a la Compañía en un **plazo máximo de 24 horas** desde el momento en que se tuvo o debió tener conocimiento de este.

- **Gestión de identidad y control de accesos:** Garantizar una adecuada gestión y registro de los accesos y permisos, en línea con el principio del mínimo privilegio, contando con las correspondientes revisiones periódicas, así como con una gestión de credenciales y métodos de acceso seguro (contraseñas robustas, MFA, etc.). Cualquier cambio en los accesos a los sistemas de la Compañía deben ser notificados. En el caso de Proveedores que accedan a los sistemas de control se requerirá una previa autorización de acceso por parte de la Compañía.

- **Gestión de la información y sus soportes:** Contar con medidas de clasificación y protección físicas y lógicas para los soportes y recursos según la criticidad y el grado de confidencialidad de la información, tener procedimientos de control y cifrados cuando aplique. Así mismo, disponer un proceso de custodia y registros/logs que identifiquen cualquier evento de seguridad.

- **Gestión de las copias de seguridad:** Disponer un procedimiento de copias de seguridad en base a las necesidades de disponibilidad del negocio, monitorizando su correcta ejecución, realizando pruebas de recuperación, y contar con un plan de continuidad de servicios TI que cubra los sistemas y centros de procesamiento de datos con los que se provee el servicio a la Compañía. En el caso de Proveedores que realicen trabajos para el sistema de control se requerirá cumplir con los procedimientos correspondientes de la Compañía.

- **Control de la cadena de suministro de terceras partes:** En el caso de subcontratar, en parte o todo, el servicio con otras entidades se deberá informar previamente a la Compañía, así como asegurar que las otras entidades cumplan con las regulaciones de seguridad, privacidad y las mismas medidas indicadas para el Proveedor.

- **Devolución y supresión de la información:** Contar con procedimiento de destrucción segura de información y dispositivos, utilizando medidas físicas y lógicas que aseguren el borrado de los datos (p.e. certificados homologados).

- **Amenazas informáticas:** Disponer de sistemas que permitan la detección y respuesta a vulnerabilidades y amenazas a riesgos de seguridad, internas y/o externas, incluyendo, por ejemplo, sistemas de protección contra malware, elementos de seguridad en las comunicaciones como firewall.