REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA TERCEROS Y PROVEEDORES

1. OBJETIVO

Establecer requisitos generales de seguridad de la información para terceros que acceden o interactúan con sistemas, redes, aplicaciones, servidores, información u otros recursos de la organización. El objetivo es reducir riesgos de acceso no autorizado, uso indebido, compromiso de credenciales, exposición de información y propagación de amenazas externas.

2. ALCANCE

Aplica a proveedores, contratistas, consultores y prestadores de servicios que requieran conectividad, acceso remoto o interacción autorizada con activos de información o recursos tecnológicos. Los controles se aplican proporcionalmente según la criticidad del servicio, el nivel de acceso, la información procesada, la exposición y el impacto potencial.

3. PRINCIPIOS GENERALES

- Autorización previa para los accesos remotos de terceros mediante solicitud formal y las aprobaciones correspondientes.
- Identidades individuales y trazables.
- Mínimo privilegio.
- Autenticación multifactor para accesos remotos.
- Vigencia limitada mientras exista una necesidad de negocio válida.
- Controles proporcionales al riesgo y capacidad de prevención y respuesta.

4. OBLIGACIONES DEL TERCERO

- Utilizar los accesos exclusivamente para la actividad aprobada.
- Proteger las credenciales y mecanismos de autenticación; no compartir cuentas.
- No intentar acceder a recursos no autorizados.
- Mantener condiciones generales de seguridad en los dispositivos utilizados.
- Permitir, cuando corresponda, la validación general de seguridad del dispositivo.
- Comunicar sospechas de compromiso o incidentes y colaborar con la contención y remediación.

5. GESTIÓN Y APROBACIÓN DE ACCESOS

Todo acceso debe originarse mediante los canales corporativos establecidos y contar con la aprobación del responsable interno. Antes de habilitarlo, se debe identificar al tercero, la necesidad de negocio, el alcance solicitado y el responsable del acceso.

Regla de control: La aprobación de la relación comercial no autoriza por sí sola el acceso a recursos tecnológicos.

6. SEGURIDAD DEL ACCESO REMOTO

Cuando el nivel de riesgo lo requiera, la organización podrá validar mediante checklist las condiciones generales de seguridad del dispositivo. La revisión puede considerar la vigencia y actualización del entorno tecnológico utilizado, la implementación de mecanismos de protección frente a amenazas, la aplicación de controles de seguridad del dispositivo y otras medidas orientadas a preservar la confidencialidad, integridad y disponibilidad de la información. La habilitación podrá condicionarse a la corrección de observaciones.

Los terceros deben utilizar identidades individuales y trazables. Se debe evitar, en la medida de lo posible, el uso de cuentas genéricas o compartidas. Los permisos se restringen a los recursos necesarios y al propósito aprobado, aplicando mínimo privilegio y segregación de funciones cuando corresponda.

7. MONITOREO Y DETECCIÓN DE AMENAZAS

La organización realiza actividades de monitoreo y detección de amenazas relacionadas con los accesos y la conectividad de terceros. Las situaciones identificadas pueden dar lugar a medidas preventivas o correctivas, incluyendo, cuando corresponda, el bloqueo temporal o la suspensión de la conectividad hasta que el riesgo haya sido evaluado y mitigado.

8. GESTIÓN DE INCIDENTES

Ante una amenaza o posible compromiso, la organización puede coordinar con el tercero la validación, contención y remediación. Según el riesgo, las medidas pueden incluir el cambio o la revocación de credenciales, la suspensión temporal del acceso, el bloqueo preventivo y el restablecimiento una vez mitigado el riesgo.

9. INCUMPLIMIENTO, REVISIÓN Y MEJORA

El incumplimiento de las obligaciones, requisitos de seguridad o condiciones de acceso establecidas en el presente lineamiento puede generar restricciones de privilegios, cambio o revocación de credenciales, suspensión o deshabilitación del acceso, bloqueo preventivo y solicitud de remediación. La continuidad o el restablecimiento quedan sujetos a la mitigación del riesgo y a la vigencia de la necesidad de negocio.

La organización revisa periódicamente la pertinencia de los accesos otorgados a terceros y ajusta las medidas de seguridad cuando cambian la necesidad de negocio, el alcance o el nivel de riesgo asociado.