Política de Seguridad en la Relación con Proveedores

Tecnología de la Información

Estrategia y Control de Gestión

Cód.: ESCG-PO-12-3

Elaborado por:	Aprobado por:	Fecha Liberación:	Fecha Próxima Actualización:
Jefe de Ciberseguridad	Gerente de administración y finanzas	10/10/2021	10/10/2024

INDICE

1. Introducción.

Esta política define y establece un conjunto de directrices de seguridad en la relación con proveedores, las cuales los colaboradores deben cumplir y aplicar con el objeto de asegurar el uso adecuado y protección de los activos de información de Esmax.

2. Objetivo.

Determinar directrices de seguridad en la relación con proveedores.

3. Alcance.

Aplicable a todos los proveedores, colaboradores y personal externo con acceso a información, sistemas, impresos y equipos de Esmax.

4. Responsabilidades.

4.1 Compete a la Gerencia de Estrategia y Control de Gestión de Esmax

- Aprobar esta política.
- Definir al responsable por la gestión de esta política.

4.2 Compete al Jefe de Ciberseguridad

- Administrar esta política, lo que incluye su desarrollo, implantación, control, evaluación y mejora continua.
- Obtener la aprobación de esta política.
- Cumplir la actividad de revisión y actualización de esta política.
- Identificar necesidades de capacitación respecto del contenido de la presente Política.
- Promover las acciones necesarias para la divulgación y aplicación de este documento.

4.3 Compete a las áreas del Negocio y colaboradores

- Cumplir la Política.
- Reportar al gerente inmediato superior y a la Jefatura de Ciberseguridad, los incidentes de seguridad donde se vean involucrados proveedores.

4.4 Compete área de Auditoría

- Revisar anualmente el cumplimiento de la política.
- Identificar, comunicar y dar seguimiento a las no conformidades derivadas del incumplimiento de la presente política.

4.5 Compete al Proveedor

- Mantenerse alineados con condiciones del anexo de presente política, la cual exige el cumplimiento de los controles parcial o total de acuerdo con la criticidad del servicio.

5. Política.

Esmax ha establecido medidas de seguridad que abarcan a toda la organización y que buscan proteger la disponibilidad, confiabilidad e integridad de la información de conformidad con su Sistema de Gestión de Seguridad de la Información (SGSI). Por ello, Esmax ha definido la siguiente Política de seguridad en la relación con Proveedores.

Esta Política aborda específicamente el Acceso de los proveedores a los activos de información de Esmax y establece obligaciones y deberes, más allá del ámbito contractual, para ambas partes respecto del uso de dichos activos.

En virtud de lo anterior, Esmax se compromete a dar a conocer clara y oportunamente las normas y procedimientos de seguridad relacionados con los “activos de información” a los que tendrán acceso los proveedores, prestando asesoría en la comprensión de dichos requisitos y aplicando los controles necesarios para su cumplimiento. También se compromete a ofrecer retroalimentación adecuada en relación con el nivel de cumplimiento y a orientar de potenciales medidas correctivas.

Los proveedores deberán:

- Acatar y dar cumplimiento a toda política, procedimiento y norma o instrucción emitido por Esmax con respecto al acceso a la información y las prácticas para resguardarlos.
- Previo a la ejecución de los servicios el proveedor deberá cumplir con las condiciones establecidas en el Anexo A del presente documento, asimismo deberá proporcionar la evidencia que permita asegurar el cumplimiento de las disposiciones establecidas en dicho anexo.
- Acatar y dar cumplimiento a las directrices o mandatos establecidos por el Jefe de Ciberseguridad.
- Respetar la confidencialidad de la información a la que tienen acceso no divulgando ningún tipo de información según la clasificación de la información dictada por Esmax, a terceros no autorizados.
- Resguardar la integridad y asegurar la disponibilidad de la información a la que tengan acceso o que dependa de ellos.
- Adherir a los controles y revisiones que determine Esmax para verificar el nivel de cumplimiento de las normas y procedimientos aplicables.
- Participar del ciclo de mejora continua cuando se detecten incumplimientos o infracciones a esta Política o procedimientos relacionados.
- Difundir entre el personal que interactúa con Esmax su adherencia a esta Política e implementar controles internos para asegurarla.
- Para todos los casos donde haya tratamiento de datos sensible, el proveedor deberá ceder Privilegios de propiedad de los datos a la Gerencia de Administración y Finanzas de Esmax.
- Debe brindar acceso al repositorio o bóveda de las llaves de cifrado y credenciales administrativas a un usuario asignado por Esmax como custodia del mismo.

Previo a que los proveedores ejecuten sus servicios se debe establecer, documentar y firmar un contrato de prestación de servicios que considere:

- Sera responsabilidad del área de compras incluir en todos los contratos la cláusula de cumplimiento de esta política.
- Sera responsabilidad del área contratante, validar con el jefe de ciberseguridad el grado de acceso a información de Esmax, de igual manera deberá informar al área de compras esta condición para que sea incluida en el anexo (a) de esta política.
- Se debe informar a la Gerencia de Administración y Finanzas todo proveedor que se adhiera a esta política y tenga acceso a información confidencial o Sistemas críticos para Esmax.
- Todo proveedor debe cumplir con los controles mínimos exigidos en el anexo A.
- Sera responsabilidad de la Gerencia de Administración y Finanzas y la Jefatura de Ciberseguridad, determinar los controles avanzados que debe adherir el proveedor y verificar según corresponda la evidencia del cumplimiento de los mismos.
- Se debe formalizar un acuerdo de confidencialidad que resguarde la información de Esmax, a la cual tendrá acceso el proveedor, en el desarrollo del servicio. Dicho acuerdo se debe formalizar previo al desarrollo y ejecución del servicio.

Durante la prestación del servicio se debe:

- Verificar periódicamente que el proveedor mantiene las condiciones de seguridad de la información, que le permitan entregar el servicio contratado en los términos acordados.
- Verificar periódicamente que el proveedor externo cumple con el acuerdo de nivel de servicios (SLA).
- Revisar las actividades que haya realizado el proveedor externo, de modo de detectar cualquier acción que pudiera representar un riesgo para Esmax.
- Será responsabilidad del contratante del servicio ejecutar auditorías al proveedor, cuando se estime conveniente.

Al término del contrato se debe asegurar:

- La coordinación de la recuperación de los activos y la información que pudiera estar en poder del proveedor, junto con ello eliminar los permisos de acceso tanto lógicos como físicos, que se hayan asignado por efectos de la relación comercial. Será responsabilidad de la Gerencia de TI, eliminar los accesos del proveedor cuando corresponda, para ello, el área contratante del servicio deberá notificar a la Gerencia de Administración y Finanzas el período de vigencia de los accesos del proveedor considerando el contrato adscrito.

Los proveedores serán responsables del cumplimiento de esta Política como organización y del cumplimiento de esta por parte de sus empleados.

Esta Política será revisada en busca de mejoras, actualizada y difundida según corresponda por el Jefe de Ciberseguridad y se considera parte integral de nuestro compromiso con el Sistema de Gestión de Seguridad de la Información.

6. Frecuencia de Revisión y Actualización de la Política.

El presente procedimiento será revisado periódicamente en función de las necesidades y actualizado cada año, a partir de su entrada en vigencia, por el jefe de ciberseguridad, quien propondrán los cambios tanto de forma como de fondo correspondientes."

7. Control de Cambios.

Versión	Fecha Modificación	Aspectos Modificados
001	6-10-2020	Creación de documento
002	10-10-2021	Control de cambio, se agregan 2 lineamientos con respecto a proveedores, tratamiento de llaves, credenciales y privilegios de admin los datos.
003	26-07-2023	Actualización de gerencia responsable.

8. Anexos.

a. Condiciones que deben cumplir los proveedores.

Previo a ejecutar las actividades contratadas por Esmax, el proveedor deberá cumplir con las condiciones de seguridad detalladas en las siguientes secciones. El cumplimiento de los controles es parcial o total de acuerdo con la criticidad del servicio, o si el proveedor accede a información confidencial, al respecto, tales criterios se especifican a continuación:

- Si el proveedor no accede a información confidencial de Esmax, o el servicio no es considerado por la organización como crítico, el proveedor deberá cumplir únicamente con aquellos controles señalados como “Control Mínimo”.

- Si el proveedor accede a información confidencial de Esmax, o el servicio es considerado por la organización como crítico, el proveedor deberá cumplir todos los controles (Controles avanzados y mínimos).

Las excepciones al cumplimiento de controles serán de responsabilidad del comité de seguridad o del Jefe de Ciberseguridad.

Respecto a normas de Ciberseguridad

Control que debe tener el proveedor	Tipo de Control	Criterio de aplicación	Evidencia
Leer y firmar adhesión de política de **"Seguridad de la información"** de Esmax.	Control mínimo	Control aplica para todo proveedor con acceso a sistemas, información o infraestructura de Esmax	Acta firmada por personal del proveedor, ejecutor del servicio, que señale la lectura, comprensión, adhesión y aplicación de la política de referencia.
Leer y firmar adhesión de política de "**Uso de Dispositivos Móviles"** de Esmax.	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas, información o infraestructura de Esmax	
Leer y firmar adhesión de política de **"Ciberseguridad para Teletrabajo"** de Esmax.	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas, información o infraestructura de Esmax	
Leer y firmar adhesión de política de **"Criptografía"** de Esmax.	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas, información o infraestructura de Esmax	
Leer y firmar adhesión de política de **"Gestión de incidentes"** de Esmax.	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas, información o infraestructura de Esmax	
Leer y firmar adhesión de política de **"Uso Aceptable de activos"** de Esmax.	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas, información o infraestructura de Esmax	
Leer y firmar adhesión de política de **"Control de acceso"** de Esmax.	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas, información o infraestructura de Esmax	
Leer y firmar adhesión de política de **"Escritorio Limpio"** de Esmax.	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas, información o infraestructura de Esmax	
Leer y firmar adhesión de política de **"Adquisición, Mantenimiento de Infraestructura y Desarrollo"** de Esmax.	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas, información o infraestructura de Esmax	

Respecto a la estación de trabajo del proveedor:

Control que debe tener el proveedor	Tipo de Control	Criterio de aplicación	Evidencia
Antivirus instalado y Actualizado en la estación de trabajo	Control mínimo	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Captura de pantalla

Control que debe tener el proveedor	Tipo de Control	Criterio de aplicación	Evidencia
Software base licenciado en la estación de trabajo	Control mínimo	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Captura de licencia
Firewall de Estación de trabajo	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Captura de pantalla
Candado de laptop	Control mínimo	Control aplica para todo proveedor que trabaje en dependencias de Esmax	Fotografía
Solución de cifrado de Disco duro	Control Avanzado	Control aplica para todo proveedor que trabaje con información confidencial de Esmax	Captura de pantalla
Sistema Data los prevention corporativo	Control Avanzado	Control aplica para todo proveedor que trabaje con información confidencial de Esmax	Captura de pantalla

Respecto del software en la estación de trabajo del proveedor:

Control que debe tener el proveedor	Tipo de Control	Criterio de aplicación	Evidencia
Software de operación licenciado	Control mínimo	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Captura de licencias
Ausencia de software de escaneo de puertos o descubrimiento de vulnerabilidades.	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Captura de pantalla
VPN autorizada por Esmax	Control mínimo	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Captura de pantalla

Respecto de control de acceso lógico y físico:

Control que debe tener el proveedor	Tipo de Control	Criterio de aplicación	Evidencia
Utilizar credencial visible	Control mínimo	Control aplica para todo proveedor que trabaje en dependencias de Esmax	Control será sancionado mediante revisiones dispuestas por Esmax en la oportunidad que se estime conveniente.

Control que debe tener el proveedor	Tipo de Control	Criterio de aplicación	Evidencia
No ingresar a dependencias no autorizadas	Control mínimo	Control aplica para todo proveedor que trabaje en dependencias de Esmax	Control será sancionado mediante revisiones dispuestas por Esmax en la oportunidad que se estime conveniente.
No manipular ningún activo de Esmax, sin existir autorización explicita por la contraparte válida.	Control mínimo	Control aplica para todo proveedor que trabaje en dependencias de Esmax	Control será sancionado mediante revisiones dispuestas por Esmax en la oportunidad que se estime conveniente.
No registrar credenciales en ningún medio (físico o digital), no autorizado por Esmax	Control mínimo	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Control será sancionado mediante revisiones dispuestas por Esmax en la oportunidad que se estime conveniente.
No compartir credenciales de los sistemas de Esmax	Control mínimo	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Control será sancionado mediante revisiones dispuestas por Esmax en la oportunidad que se estime conveniente.
No ejecutar herramientas de hacking en la red de Esmax (ejemplo; nmap, nessus, metaexploit,etc)	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Control será sancionado mediante revisiones dispuestas por Esmax en la oportunidad que se estime conveniente.
No publicar servicios, puertos y protocolos de comunicaciones no autorizados (ejemplo: Telnet, FTP, HTTP, etc)	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Control será sancionado mediante revisiones dispuestas por Esmax en la oportunidad que se estime conveniente.
No modificar mecanismos de control de acceso sin autorización (reglas de FW, perfiles, privilegios, etc)	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Control será sancionado mediante revisiones dispuestas por Esmax en la oportunidad que se estime conveniente.
No instalar sistemas en entornos productivos sin autorización.	Control Avanzado	Control aplica para todo proveedor con acceso a sistemas o infraestructura de Esmax	Control será sancionado mediante revisiones dispuestas por Esmax en la oportunidad que se estime conveniente.

9. Registros.

Identificación	Almacenamiento	Grado de sigilo	Protección	Recuperación	Tiempo de Retención	Descarte
Política de Seguridad en la Relación con Proveedores.	Electrónico.	Corporativo.	Acceso al sistema por clave y contraseña y Sistema protegido por backup.	Procedimientos almacenados por código.	Permanente.	N/A