Política de Protección de la información

Por Ángel Morales Botello
Cybersecurity Manager
IT Research & Development Department

Ciudad de México, septiembre de 2023

Tabla de contenido

OBJETIVO

La política de Protección de la Información tiene como objetivo establecer directrices y prácticas para garantizar la confidencialidad, integridad y disponibilidad de la información almacenada y procesada en los sistemas informáticos de Vesta. Esta política se centra en el establecimiento de controles de acceso, medidas de seguridad y copias de seguridad para proteger la información crítica de la organización.

ALCANCE

Esta política se aplica a todos los empleados, contratistas y terceros que trabajen con los sistemas y activos de la empresa.

CONTROLES DE ACCESO

Se establecerán controles de acceso para garantizar que la información confidencial solo sea accesible por personal autorizado.

Se implementarán medidas de autenticación adecuadas, como contraseñas seguras y autenticación multifactor para verificar la identidad de los usuarios.

Los derechos de acceso se asignarán de manera basada en el principio mínimo de privilegio, el cual se definirá en la matriz de segregación de funciones que se trabajará en conjunto con cada área y recursos humanos, asegurando que los usuarios tengan acceso solo a la información requerida para llevar a cabo sus responsabilidades laborales.

Se realizará una revisión periódica de los derechos de acceso para garantizar que se mantenga la consistencia con las responsabilidades laborales de los usuarios.

INTEGRIDAD Y CONFIDENCIALIDAD DE LOS DATOS

Se establecerán medidas de seguridad para garantizar la integridad y confidencialidad de los datos almacenados en los sistemas informáticos.

Se utilizarán técnicas de cifrado para proteger los datos confidenciales tanto en tránsito como en reposo.

Los sistemas informáticos y las aplicaciones críticas serán regularmente parcheados y actualizados para mitigar vulnerabilidades y mantener su integridad y seguridad.

Se implementarán sistemas de prevención de pérdida de datos (DLP) y monitoreo de seguridad para detectar y prevenir amenazas internas y externas a la integridad y confidencialidad de los datos.

RESPONSABILIDADES

El equipo de Ciberseguridad será responsable de implementar y mantener actualizada la política de Protección de la información.

Todos los empleados, contratistas y terceros que trabajen con los sistemas y activos de la empresa, incluyendo los dueños de la información, serán responsables de cumplir con las políticas y procedimientos establecidos en esta política. La colaboración activa de los dueños de la información es esencial para garantizar un enfoque integral y eficaz para la seguridad de la información en toda la organización.

ACTUALIZACIÓN DE LA POLÍTICA

Esta política será revisada y actualizada anualmente por el equipo de Ciberseguridad para garantizar que se mantenga al día con las mejores prácticas y las necesidades de la empresa.

Cualquier cambio en esta política será comunicado a todos los empleados, contratistas y terceros que trabajen con los sistemas de la empresa.

Todos los empleados, contratistas y terceros deberán leer y firmar una declaración de aceptación de la política de gestión de parches y actualizaciones de la empresa antes de trabajar con los sistemas de la empresa.

EXCEPCIONES

En una política de ciberseguridad enfocada en la protección de la información, las excepciones suelen ser situaciones que requieren un tratamiento especial de los datos o una desviación de las normas estándar para facilitar operaciones críticas o cumplir con obligaciones legales. Algunas excepciones posibles podrían incluir:

1. Divulgación Autorizada por Ley:
   Situaciones donde la organización está legalmente obligada a revelar información confidencial o sensible, como en respuesta a citaciones judiciales, requerimientos legales o investigaciones gubernamentales.

2. Compartir Información para Fines de Colaboración:
   Intercambio de datos críticos con socios de confianza, aliados estratégicos o en el marco de acuerdos de colaboración interinstitucional, donde dicho intercambio es vital para la misión de la organización pero se realiza bajo estrictos acuerdos de confidencialidad.

3. Excepciones para Personal de Alto Nivel o Roles Específicos:
   Directivos o empleados en roles críticos que puedan necesitar un acceso más amplio a la información o la capacidad de compartir datos de manera más flexible para tomar decisiones estratégicas importantes.

4. Investigación y Desarrollo:
   Excepciones para el personal de I+D que trabaja en proyectos innovadores y que puede necesitar acceso a información protegida o la capacidad de utilizarla de manera no convencional, siempre dentro de un marco controlado.

5. Acceso de Emergencia:
   Situaciones de emergencia donde es necesario acceder a información restringida para resolver problemas urgentes que afectan a la operatividad o seguridad de la organización.

6. Transferencia de Datos a través de Fronteras:
   En el contexto de operaciones globales, la transferencia internacional de datos puede requerir excepciones debido a las diferencias en las leyes de protección de datos entre países, aunque siempre se debe buscar cumplir con los marcos legales como el GDPR en la Unión Europea.

7. Copias de Seguridad y Archivo:
   Excepciones para el manejo de copias de seguridad y datos archivados, que podrían requerir un nivel diferente de protección o ser almacenados en ubicaciones que normalmente no se utilizan para datos activos.

8. Uso de Datos para Capacitación y Pruebas:
   Uso de datos reales en entornos de prueba o capacitación, donde normalmente se requeriría despersonalizar la información, pero bajo ciertas condiciones controladas se permite el uso de datos auténticos.

Para cada excepción, es crucial que existan procedimientos claros para la solicitud, aprobación y registro, asegurando que se manejen de manera transparente y con las salvaguardas necesarias para minimizar los riesgos. Además, debe haber una revisión periódica de las excepciones para garantizar su relevancia y necesidad continuas.

CONCLUSIÓN

Esta política proporciona directrices claras para proteger la información crítica de la organización, incluyendo el establecimiento de controles de acceso, medidas de seguridad y prácticas de copia de seguridad. La seguridad de la información es fundamental para Vesta, y esta política garantiza su protección adecuada.