




# Política General de Ciberseguridad


Por Ángel Morales Botello  
Cybersecurity Manager  
IT Research & Development Department

Ciudad de México, septiembre de 2023

 - Confidencial -	Política de Ciberseguridad	Versión	Fecha validez	Fecha próxima revisión
	<i>Estrategia TechSafe 1 Vesta</i>	1.0	2023	2024

## Tabla de contenidos

INTRODUCCIÓN.....	3
OBJETIVOS Y ALCANCE.....	3
ROLES Y RESPONSABILIDADES .....	3
PROTECCIÓN DE LA INFORMACIÓN.....	3
ACCESO Y AUTENTICACIÓN .....	4
PROTECCIÓN DE DISPOSITIVOS .....	4
USO ACEPTABLE DE LOS SISTEMAS INFORMÁTICOS .....	4
USO DE CORREO ELECTRÓNICO E INTERNET .....	5
CAPACITACIÓN Y CONCIENCIACIÓN DE SEGURIDAD .....	5
GESTIÓN DE INCIDENTES DE SEGURIDAD.....	5
CUMPLIMIENTO Y AUDITORÍA.....	5
GESTIÓN DE PROVEEDORES .....	6
MONITOREO Y DETECCIÓN DE AMENAZAS.....	6
DISPOSITIVOS PERSONALES (BYOD).....	6
PARCHES Y ACTUALIZACIONES.....	6
PROTOCOLOS DE CIFRADO DE INFORMACIÓN .....	6
CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES.....	7
CONCLUSIÓN .....	7
APROBACIONES.....	7

 - Confidencial -	Política de Ciberseguridad	Versión	Fecha validez	Fecha próxima revisión
	<i>Estrategia TechSafe 1 Vesta</i>	1.0	2023	2024

## INTRODUCCIÓN

La seguridad de la información es fundamental para el éxito de cualquier empresa moderna. La presente política establece los estándares y procedimientos necesarios para garantizar la seguridad de la información en nuestra empresa. Los colaboradores, contratistas y terceros que utilicen los recursos de la empresa deben cumplir con esta política y mantener una postura de seguridad activa y constante.

## OBJETIVOS Y ALCANCE


1. Salvaguardar la información crítica de la empresa, incluyendo datos de clientes, propiedad intelectual, información financiera y estratégica.
2. Proteger los recursos de tecnología de la información de la empresa, incluyendo hardware, software, redes y sistemas.
3. Desarrollar planes (BCP y DRP) que ayuden a garantizar en el futuro, en un alto porcentaje, la continuidad del negocio y la disponibilidad de los recursos tecnológicos de la empresa en caso de interrupciones por ataques.
4. Trabajar en el cumplimiento de las leyes (Ley Mexicana) y regulaciones aplicables y mantener la confidencialidad, integridad y disponibilidad de la información.
5. Crear planes de trabajo para lograr en un periodo razonable la certificación ISO 27001.

## ROLES Y RESPONSABILIDADES

1. La alta gerencia es responsable de garantizar que la seguridad de la información se considere en todas las decisiones donde datos sensibles se vean involucrados y se asignen los recursos necesarios.
2. El Cybersecurity Manager es responsable de desarrollar, implementar y mantener la política de seguridad de la información.
3. Los gerentes son responsables de garantizar que los colaboradores a su cargo cumplan con esta política y que se tomen las medidas necesarias para garantizar la seguridad de la información.
4. Los colaboradores son responsables de cumplir con esta política y tomar medidas para proteger la información y los recursos de la empresa.

## PROTECCIÓN DE LA INFORMACIÓN

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

 - Confidencial -	Política de Ciberseguridad	Versión	Fecha validez	Fecha próxima revisión
	<i>Estrategia TechSafe 1 Vesta</i>	1.0	2023	2024

2. Establecer medidas de seguridad para garantizar la integridad y confidencialidad de los datos almacenados en los sistemas informáticos.
3. Se realizarán copias de seguridad periódicas de la información crítica.

## ACCESO Y AUTENTICACIÓN


1. Los colaboradores solo tienen acceso a los recursos necesarios para realizar sus funciones laborales.
2. Los colaboradores deben usar contraseñas seguras y cambiarlas regularmente. Las contraseñas deben contener al menos 12 caracteres, incluidos números, letras mayúsculas y minúsculas, y símbolos.
3. Los colaboradores no deben compartir contraseñas ni permitir que otras personas usen sus cuentas.
4. La autenticación multifactor (MFA) es obligatoria para todos los usuarios que acceden a los recursos de la empresa.

## PROTECCIÓN DE DISPOSITIVOS

1. Todos los dispositivos electrónicos, incluyendo laptops y celulares, deben contar con un software de protección contra virus y malware, y con las últimas actualizaciones de seguridad.
2. Se deben configurar los dispositivos para que se bloqueen automáticamente después de un período de inactividad, y se deben implementar medidas de autenticación fuerte para el acceso a los dispositivos y datos sensibles.

## USO ACEPTABLE DE LOS SISTEMAS INFORMÁTICOS

1. Establecer reglamentos y procedimientos para garantizar el uso apropiado de los sistemas informáticos de la empresa.
2. Prohibir el uso no autorizado de los sistemas informáticos, como el uso de software no autorizado.

 - Confidencial -	Política de Ciberseguridad	Versión	Fecha validez	Fecha próxima revisión
	<i>Estrategia TechSafe 1 Vesta</i>	1.0	2023	2024

## USO DE CORREO ELECTRÓNICO E INTERNET

1. Los colaboradores y terceros deben utilizar el correo electrónico y el acceso a Internet de manera responsable y únicamente para fines empresariales legítimos.
2. Los usuarios deben evitar el acceso a sitios web inseguros o desconocidos, y se deben bloquear los correos electrónicos de spam y phishing.

## CAPACITACIÓN Y CONCIENCIACIÓN DE SEGURIDAD


1. Se proporcionará capacitación regular a todos los colaboradores sobre la importancia de la seguridad de la información y la forma de protegerla.
2. Se fomentará la conciencia sobre ciberseguridad entre todos los colaboradores.

## GESTIÓN DE INCIDENTES DE SEGURIDAD

1. Establecer procedimientos para la notificación y gestión de los incidentes de seguridad.
2. Realizar investigaciones y análisis de los incidentes de seguridad para identificar las causas y prevenir futuros incidentes similares.
3. Esta política de ciberseguridad se revisará y actualizará periódicamente para garantizar que siga siendo efectiva y se adapte a los cambios en la tecnología y los riesgos de seguridad. Además, se establecerá un programa de auditoría para evaluar la efectividad de los controles de seguridad y garantizar el cumplimiento de esta política de ciberseguridad.

## CUMPLIMIENTO Y AUDITORÍA

1. Llevar a cabo auditorías periódicas para evaluar el cumplimiento de esta política de ciberseguridad.
2. Los resultados de las auditorías se utilizarán para identificar áreas de mejora y tomar medidas correctivas según corresponda.
3. Realizar pruebas de penetración para evaluar la seguridad de los sistemas informáticos de la empresa.
4. La política de ciberseguridad se actualizará periódicamente para mantenerse al día con las mejores prácticas y los cambios regulatorios.

 - Confidencial -	Política de Ciberseguridad	Versión	Fecha validez	Fecha próxima revisión
	<i>Estrategia TechSafe 1 Vesta</i>	1.0	2023	2024

## GESTIÓN DE PROVEEDORES

1. Establecer medidas de seguridad para garantizar que los proveedores de servicios y productos de tecnología cumplan con los requisitos de seguridad establecidos en esta política de ciberseguridad.
2. Llevar a cabo una evaluación de riesgos de los proveedores para identificar posibles riesgos de seguridad y tomar medidas preventivas.

## MONITOREO Y DETECCIÓN DE AMENAZAS

1. Establecer procedimientos para el monitoreo y detección de amenazas en la empresa.
2. Los procedimientos se revisarán y actualizarán periódicamente para garantizar que sigan siendo efectivos y estén actualizados.

## DISPOSITIVOS PERSONALES (BYOD)


1. Queda estrictamente prohibido el uso de dispositivos personales para acceder a los sistemas, redes y recursos de la empresa.
2. Todos los colaboradores deben utilizar únicamente dispositivos corporativos o aquellos proporcionados y gestionados por la empresa para acceder a los recursos de TI.

## PARCHES Y ACTUALIZACIONES

1. Establecer una política y procedimientos para la gestión de parches y actualizaciones a los sistemas de la empresa.
2. Los procedimientos se revisarán y actualizarán periódicamente para garantizar que sigan siendo efectivos y estén actualizados.

## PROTOCOLOS DE CIFRADO DE INFORMACIÓN

1. Establecer una política y procedimientos para los protocolos de cifrado de información confidencial de la empresa.
2. Los procedimientos se revisarán y actualizarán periódicamente para garantizar que sigan siendo efectivos y estén actualizados.

 - Confidencial -	Política de Ciberseguridad	Versión	Fecha validez	Fecha próxima revisión
	<i>Estrategia TechSafe 1 Vesta</i>	1.0	2023	2024

## CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES

1. Establecer planes de continuidad del negocio y recuperación ante desastres para garantizar la disponibilidad de los sistemas informáticos de la empresa en caso de interrupciones.
2. Los planes se revisarán y actualizarán periódicamente para garantizar que sigan siendo efectivos y estén actualizados.

## CONCLUSIÓN

Esta política de ciberseguridad debe ser comunicada y distribuida a todos los colaboradores de la empresa. Además, establecer un proceso de seguimiento y supervisión para garantizar que todos los colaboradores cumplan con los requisitos de seguridad establecidos en esta política.

## APROBACIONES

Nombre: \_\_\_\_\_  
 Por el Consejo de Administración Firma

Nombre: \_\_\_\_\_  
 Consejero Delegado de Seguridad Informática Firma


Lorenzo Dominique Berho  
 CEO Vesta Firma

Juan Sottit Achútegui  
 CFO Vesta Firma

Iván Saavedra Maufras  
 IT Research & Development Director Firma

Ángel Morales Botello  
 Cybersecurity Manager Firma

En Ciudad de México, México, a \_\_\_\_\_  
 dd mm aaaa

 - Confidencial -	Política de Ciberseguridad	Versión	Fecha validez	Fecha próxima revisión
	<i>Estrategia TechSafe 1 Vesta</i>	1.0	2023	2024

*Este documento es el resultado del esfuerzo colaborativo y la dedicación del equipo de IT Research & Development de Vesta, cuyos miembros han aportado su experiencia y conocimientos especializados para su creación y redacción.*