POL 1 - Política general de seguridad

INFORMACIÓN DEL DOCUMENTO

Código Documento:	POL 1	**Versión**	6
Fecha de documento:	17/02/2020	**Empresa:**	Netactica
Preparado por:	Carolina Cekci	**Aprobado por:**	Oscar Encinas
Fecha de preparación:	17/02/2020	**Fecha de revisión:**	9/08/2022

CONTROL DE VERSIONES

No. Versión	Fecha Versión	Revisado por:	Descripción
1	14/04/2020	Oscar Encinas	Creación
2	09/08/2022	Oscar Encinas	Actualización
3	15/05/2023	Ariel Menéndez	Se detalla listado de acceso a tecnologías críticas
4	26/01/2024	Carolina Cekci	Actualización comité de seguridad y gestión de incidentes
5	04/03/2024	Ariel Menéndez	Se agrego “Detección e informe oportuno de fallas”
6	20/03/2024	Carolina Cekci	Se actualiza listado de tecnologías criticas y agrega texto final firma del empleado

En el desarrollo y funcionamiento de los servicios de Netactica, la información es un activo que tiene un alto valor. La Dirección de Netactica reconoce la necesidad de garantizar en todo momento la disponibilidad, integridad y confidencialidad de la información como elemento esencial para el correcto desempeño de los servicios que presta a sus clientes y para el cumplimiento de los requisitos legales vigentes. Por todo ello soporta los objetivos y principios establecidos en esta política.

El objetivo prioritario de esta política es proporcionar las directrices para la gestión de la seguridad de la información, y como consecuencia de ello, obtener el más alto nivel de garantía en el tratamiento y custodia de la información dentro de Netactica. Para conseguir estas metas, se identificarán y evaluarán permanentemente los riesgos que amenazan nuestros sistemas de información, se planificará el control y reducción de aquéllos cuando sea posible y se realizará su seguimiento constante en el resto de casos. Todo lo anterior se enmarca en un compromiso de mejora continua utilizando como marco de referencia las normas ISO 9001:2015 Y PCI DSS para establecer el sistema de gestión de la seguridad de la información y la norma ISO 9001:2015 como conjunto de buenas prácticas para la gestión de la seguridad de la información.

La Dirección muestra también su compromiso a proporcionar los medios necesarios, cuenta con la colaboración de todos los empleados y asume la responsabilidad de su concienciación y formación en materia de seguridad de la información, como medio para garantizar el cumplimiento de esta política.

Oscar Encinas

Gerente General

PROPIEDAD Y CUMPLIMIENTO

El Comité de Seguridad de la Información reconocen la importancia de la seguridad de la información en el modelo de Negocio de **NETACTICA** y con el fin de generar y mantener la ventaja competitiva y la permanencia y el valor del negocio, aprueban "Las políticas de Seguridad de la información" expuestas en el presente documento con los procedimientos y estándares que las soportan, los cuales cuentan con el respaldo del comité de seguridad.

Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deberían recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.

NETACTICA prohíbe explícitamente que el PAN (número de cuenta personal) sea enviado a través de tecnologías de mensajería de usuario final, como correo electrónico, SMS o chats etc.

El cumplimiento de las políticas de seguridad es obligatorio para todo el personal o terceros (Proveedores, contratistas y socios) que acceden o usan los sistemas de información de **NETACTICA**, por tal motivo se debe asegurar que cada uno de los actores conoce, entiende y acepta el presente documento.

La dirección deberá proveer los mecanismos y apoyar los procesos que permitirán asegurar el éxito de la presente política de seguridad de la información al interior de la compañía.

En caso de incumplimiento de la presente política de seguridad se deberán establecer las medidas sancionatorias correspondientes a la falta, de acuerdo a su criticidad y recurrencia. Éstas bien pueden ser medidas legales o contractuales con la parte involucrada.

- Éste documento así como toda política documentada debe ser revisada y actualizada con una periodicidad mínima de una (1) vez al año o cuando ocurran cambios significativos en la infraestructura o en la normatividad.
- **NETACTICA** establece un programa para mantener el cumplimiento de PCI-DSS y sus controles en la empresa para mantener los controles de seguridad.
- **NETACTICA** implementa mecanismos para la detección e informe de fallas de los sistemas críticos de control de seguridad de la entidad.

Toda documentación relacionada con las Políticas de Seguridad de la Información es aprobada por el Comité de Seguridad de **NETACTICA** y comunicada a todos los usuarios.

En caso de aplicar una modificación o cambio en las políticas generales, se requiere de la aprobación del Comité de Seguridad de Información de **NETACTICA** para su implantación y posterior cumplimiento.

Violaciones a la política

Cualquier empleado que sea encontrado violando la política de seguridad en la Organización, será sometido a acciones de tipo disciplinario, que pueden incluir, más no estar limitadas a:

- Acción de tipo disciplinario según los lineamientos establecidos por el Código Sustantivo del Trabajo, el Reglamento Interno de Trabajo, las Cláusulas Especiales que se establezcan con los empleados en sus Contratos Laborales y/o todo aquello que según las leyes colombianas definen como acciones disciplinarias patronales.
- Suspensión o acceso restringido a las áreas de procesamiento de la información.
- Terminación del contrato de trabajo o relación comercial (Basados en las disposiciones emitidas por las leyes colombianas en materia laboral).

GENERALIDADES

NETACTICA Reconoce la importancia de la información como un activo al interior de la organización así como la seguridad de la misma, en busca del cumplimiento normativo y la protección de los datos que nuestros clientes nos han confiado, se han implementado una serie de controles y políticas de seguridad en la compañía para asegurar los tres principios básicos de integridad, disponibilidad y confidencialidad sobre la información.

Los lineamientos principales son la identificación, autenticación y el control de acceso físico y lógico, desarrollo de aplicaciones seguro, gestión de recursos humanos, Gestión de riesgos e incidentes de seguridad.

Toda la información contenida en el presente documento es de uso exclusivo de **NETACTICA** y no debe ser duplicada total o parcialmente o liberada a una tercera parte sin una previa autorización.

NETACTICA es una empresa líder en Latinoamérica en el desarrollo de software para el sector de viajes y turismo, uno de sus objetivos es ser el mejor socio estratégico de las agencias de viajes, operadores, mayoristas, distribuidores y líneas aéreas, promueve los diferentes servicios relacionados con turismo.

OBJETIVOS

- Desarrollar y mantener las políticas de seguridad que buscan asegurar la integridad, disponibilidad y confidencialidad de la información digital y física existente en los sistemas y procesos de **NETACTICA**
- Dar confiabilidad a nuestros clientes
- Mejorar procesos.
- Mantener los clientes que se tienen y atraer nuevos clientes.

ALCANCE

Todas las personas contratadas, proveedores y contratistas que accedan o hagan uso de los sistemas de información de **NETACTICA**

Estas políticas deben ser conocidas, aceptadas y usadas por todas las partes involucradas.

GLOSARIO

Autenticación: Procedimiento informático que permite asegurar que un usuario de un sitio web u otro servicio similar es auténtico o quien dice ser.

Autenticidad: Califica a aquello que está documentado o certificado como verdadero o seguro.

Mejora Continua: Es el conjunto de acciones dirigidas a obtener la mayor calidad posible de los productos, servicios y procesos de una empresa

Información documentada: información que una organización tiene que controlar y mantener, así como el medio en que está contenida.

Evento: Suceso imprevisto. Acontecimiento, especialmente si es de cierta importancia.

Riesgo: Posibilidad de que se produzca un contratiempo o peligro, de que algo sufra daño.

Disponibilidad: La información debe estar disponible para quien la necesita, cuando la necesita.

Integridad: La información debe ser fiable y ajustada a la realidad en todo momento.

Confidencialidad: La información debe ser consultada únicamente por aquellas personas que tienen una autorización expresada a ésta.

Componentes de sistema: Todo componente de hardware en el alcance PCI incluyendo equipos de seguridad, servidores, dispositivos de red.

Tecnologías críticas: Un sistema o tecnología que la entidad considera de particular importancia. Por ejemplo, es posible que se requiera un sistema crítico para el desempeño de una operación comercial o para mantener una función de seguridad. Algunos ejemplos de sistemas críticos generalmente incluyen sistemas de seguridad, los dispositivos y sistemas públicos, las bases de datos y otros sistemas que almacenan, procesan o transmiten datos del titular de la tarjeta.

Control de acceso: Mecanismo que limita la disponibilidad de información o de los recursos necesarios para su procesamiento sólo a personas o aplicaciones autorizadas.

- Acceso administrativo: Privilegios elevados o aumentados que se otorgan a una cuenta para que ésta administre sistemas, redes y/o aplicaciones.
- PCI-DSS: por sus siglas en ingles Payment Card Industry Data Security Standard, Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.

RESPONSABILIDADES

Alta Dirección

El equipo directivo es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la organización.

La gerencia debe apoyar el cumplimiento de la norma, validando que la operación del negocio esté alineado en todo momento con la norma PCI-DSS.

Responsable de Seguridad de la Información y cumplimiento PCI

1. Promover y participar en el desarrollo e implantación de la Política de Seguridad de la Información, normativas, procedimientos, estándares y directrices asociados a la seguridad de la información.
2. Monitorear y analizar las alertas referentes a la seguridad de la información.
3. Establecer canales de comunicación con los diferentes agentes que intervienen en la Seguridad de la Información de Netactica de manera especial con los administradores de los sistemas, técnicos de seguridad y responsables de seguridad física.

4. Colaborar en el inicio de proyectos relacionados con la Seguridad de la Información, promoviendo aquellos que pudieran cubrir las necesidades de La organización Acordar mecanismos y procedimientos específicos para proveer la seguridad requerida en cada sistema.
5. Escalar cualquier conflicto o aspecto no resuelto que afecte a varias áreas o departamentos al Comité de Seguridad de la Información.
6. Realizar periódicamente un análisis de riesgos que permita la identificación del nivel de exposición (vulnerabilidades) frente a las amenazas que afecten a La organización e identificar las opciones o líneas de actuación que permitan reducir los riesgos a un nivel aceptable.
7. Promover el cumplimiento de la norma PCI-DSS dentro de Netactica.
8. Establecer, documentar y distribuir los procedimientos de escalamiento respuesta ante incidentes que se puedan presentar al interior de Netactica y que afecten la seguridad de la información.
9. Administrar las cuentas de usuario, incluso las incorporaciones, eliminaciones y modificaciones.
10. Monitorear y analizar las alertas correspondientes a la seguridad de la información y comunicarlas al personal correspondiente.

Propietarios o Dueños de la Información

1. Identificar y aceptar la responsabilidad asociada a la información que gestionan en su ámbito de responsabilidad.
2. Promover la aplicación de las funciones y responsabilidades de los usuarios en materia de seguridad de la información y la aplicación de buenas prácticas de seguridad.
3. Clasificar la información bajo su control basado en criterios de sensibilidad y/o criticidad según lo establecido en la política de clasificación de información.
4. Identificar las necesidades de formación, en materia de seguridad de la información, en las personas que trabajan en sus áreas de responsabilidad.
5. Aprobar las solicitudes de acceso de los usuarios en sus áreas de responsabilidad y para la información de la que son responsables, apoyándose en el principio básico de necesidad de conocer dicha información.
6. Revisar periódicamente la lista de usuarios autorizados en los sistemas de información que proceden o almacenen los datos de los que los propietarios son responsables, informando de las excepciones al Responsable de seguridad de Netactica.

Funcionarios de Netactica

1. Leer y cumplir con la presente política de seguridad de la información.
2. Informar oportunamente ante cualquier evento que ponga en riesgo la seguridad de la información.
3. Cumplir con la norma PCI-DSS dentro de la organización y cuando realizan las actividades que están a su cargo.
4. Utilizar adecuadamente los accesos a los sistemas de la organización y mantener contraseñas seguras recordando que dichos accesos no se deben compartir.
5. Firmar y cumplir con el acuerdo de confidencialidad con Netactica.

Comité de Seguridad de la Información

1. Formulación, revisión y aprobación de la Política de Seguridad así como de las metodologías y procedimientos asociados al Sistema de Gestión de Seguridad de la Información (en adelante SGSI).
2. Aprobar la asignación de responsabilidades específicas dentro de Netactica relativas a la seguridad de la información.
3. Promover planes y programas de concienciación del personal en esta materia.
4. Revisar la idoneidad de los distintos controles de seguridad, facilitar los recursos necesarios y coordinar su implantación efectiva.
5. Seguimiento de las actividades desempeñadas por el Director de IT y del Comité de Seguridad así como la del resto de agentes que intervienen en la seguridad de la información.
6. Responsable de mantener el cumplimiento de PCI DSS.
7. Velar por el mantenimiento de la norma PCI-DSS y comunicar a la alta gerencia periódicamente el estado de cumplimiento al interior.

COMITÉ DE SEGURIDAD:

Ariel Menéndez Director de Tecnología Informática
Estefanía Loaiza Responsable de Seguridad de la Información
Sebastián Paladino Director Desarrollo
Johan Martin COO
Mauricio Tabares Automatizador
Carolina Cekci Dirección de auditorias

Contraseñas

Todos los funcionarios de **NETACTICA** cuentan con un usuario único y contraseña para acceder a los sistemas de la organización por lo tanto el uso de este acceso será responsabilidad de cada uno de los funcionarios y el mal uso de estos accesos podrán llevar a acciones disciplinarias graves.

Las responsabilidades de los usuarios frente al uso de sus contraseñas son:

- Utilizar contraseñas fuertes de mínimo 12 caracteres
- La contraseña debe tener: un carácter especial, una mayúscula, una minúscula y que no sea de fácil acceso por otra persona.
- El sistema no permite que se usen contraseñas iguales a las anteriores por ello no se permite el reúso de las últimas 4 contraseñas
- Es importante no compartir la contraseña con otra persona, teniendo en cuenta que el acceso está ligado a cada funcionario se revisará sus acciones teniendo en cuenta dicho acceso.
- habrá una desconexión automática de sesiones para tecnologías de acceso remoto después de un período de 15 minutos de inactividad.

Control de cambios

Entendiendo la importancia del control de cambios se ha estipulado el procedimiento mediante el cual se deben solicitar los cambios que se requieran para ejecutar las labores operativas de cada cargo.

Cada vez que se requiera solicitar un cambio se deberá crear un caso en la herramienta Asana y allí justificar el porqué, fecha en la que se requiere el cambio y el responsable de la actividad. El responsable deberá validar la viabilidad del cambio solicitado evaluando desde la funcionalidad y la seguridad de la información que no afecte ni ponga en riesgo la operación de la organización. La denegación o aprobación del mismo deberá quedar documentada en ticket creado en la herramienta de Asana.

Algunos ejemplos de cambios son: restablecimiento de contraseñas por pérdida o vulneración, habilitación de un puerto o servicio, acceso algún componente tecnológico, entre otros.

Gestión de incidentes

Una respuesta eficaz y apropiada en el caso de un incidente de seguridad puede hacer la diferencia en gastos económicas y pérdidas de información, por ello **NETACTICA** ha creado un procedimiento de respuesta a incidentes donde se estipula que cualquier empleado puede reconocer una brecha de seguridad que conlleve a un incidente por ello cualquier funcionario puede informar ante fallas o vulnerabilidades que se presenten mientras hacen sus labores diarias.

El equipo designado para la gestión de incidentes y que estará disponible en caso de ser necesario es:

COMITÉ GESTIÓN DE INCIDENTES:
Ariel Menéndez Director de Tecnología Informática
Estefanía Loaiza Oficial de seguridad de la informática
Sebastián Paladino Director Desarrollo
Mauricio Tabares Automatizador

El equipo mencionado deberá asistir a una capacitación anual donde se revise la manera adecuada de atender un incidente de seguridad y se realice actualización de las amenazas de ciberseguridad frecuentes en la industria.

- Los administradores de la información son los responsables de coordinar y administrar las respuestas contra cualquier vulnerabilidad o evento que ha sido reportado, incluyendo la documentación de los pasos tomados durante la emergencia, la recolección de evidencia y el cierre del evento.
  Se debe realizar la evaluación de gestión de riesgos al menos una vez al año o cuando existan cambios significativos.
- Establecer métricas para la cuantificación de los riesgos y su debido seguimiento en la organización.
- Implementar medidas de mitigación de riesgos así como actualización constante de amenazas informáticas en los componentes del sistema.
- Se debe realizar la revisión de los registros de auditoria (logs) de los componentes del sistema y esta debe estar alineada con la estrategia de gestión de riesgos.

Uso adecuado de tecnologías de Usuario Final

Se ha definido las tecnologías críticas como aquellos componentes que permiten la operación de la empresa pero que de ser manejados de manera errada pueden afectar la seguridad de los datos de tarjeta y confidenciales.

No es el caso de **NETACTICA**, pero si por algún motivo se tuviera acceso a datos de tarjetahabientes se prohíbe mover, copiar y almacenar CHD en discos locales y dispositivos electrónicos extraíbles.

- Se requiere que toda tecnología crítica usada en la compañía sea aprobada explícitamente por cargo.
- Todo acceso a las tecnologías críticas debe tener multi-factor de autenticación y un tiempo de desconexión automática de las sesiones establecidas por accesos remotos. Al desconectar las tecnologías de acceso remoto cuando no se utilizan, se minimizan los riesgos y el acceso a las redes.
- **NETACTICA** tiene una lista actualizada de todos los dispositivos críticos aprobados con el personal autorizado para usar estos componentes.
- Toda tecnología critica estará en las redes establecidas por **NETACTICA** las cuales están configuradas para mantener la seguridad de los datos sensibles, cualquier otro dispositivo que se conecte al entorno del negocio también debe tener configuraciones que brinden seguridad al acceder a las redes.
- Todo acceso remoto que se establezca por parte de externos de la compañía y proveedores se deben autorizar por cargo por el tiempo que se requieran hacer las actividades y luego se deben deshabilitar.
- **NETACTICA** prohíbe explícitamente cualquier tipo de extracción de información sensible en medios extraíbles, medios electrónicos o accesos remotos.

Las tecnologías críticas que se estipulan en **NETACTICA** y que son de manejo de los funcionarios se listan a continuación:

Correo electrónico

- No se deberá enviar datos de tarjeta ni información confidencial sin cifrar por este medio.

Equipos portátiles

- No deben ser utilizados por personal diferente al funcionario que se designó, debe mantener su antivirus activo y demás componentes que instale el Director de IT para el correcto funcionamiento y cuidado de la información.

Tecnologías de acceso remoto

- Solo se podrán conectar por medio de tecnologías de acceso remoto el personal que para dicho caso requiera, así mismo deberá tener autorización expresa de su jefe directo y del responsable de la seguridad de la información.

VPN

- Se requiere el uso de VPN para acceder a recursos del CDE.
- Se deben seguir las políticas de seguridad específicas al utilizar VPN, incluida la autenticación adecuada, el uso de MFA y la desconexión cuando no se esté utilizando.

MFA

- Se implementará la autenticación multifactorial en todos los sistemas que interactúen con el entorno del CDE.
- Se proporcionará formación sobre cómo configurar y utilizar adecuadamente la autenticación multifactorial para garantizar la seguridad los accesos.

Certificado de seguridad (SSL)

- Todo empleado que acceda a la consola de administración de recursos del CDE debe ser consciente de que la información se encuentra correctamente cifrada entre el navegador y la consola, validando que el certificado del proveedor se encuentra vigente y en correcto funcionamiento.

Navegador web

- Se instruirá a todos los empleados sobre las prácticas seguras de navegación web, incluida la identificación y evasión de sitios web maliciosos o no seguros que puedan los recursos pertenecientes al CDE.
- Se deben utilizar navegadores web actualizados y con parches de seguridad instalados para reducir el riesgo de explotación de vulnerabilidades.

Listado de empleados con acceso a tecnologías críticas:

A continuación detallamos el listado de los empleados con acceso a tecnologías críticas, siendo que tanto Oscar Encinas como Carolina Cekci pueden autorizar dicho acceso:

Ariel Menéndez, Director de tecnología informática, amenendez@netactica.com

Sebastián Paladino, Director de desarrollo, spaladino@netactica.com

Giovani Zago, Gerente de Desarrollo y Aplicaciones, gzago@netactica.com

Julián Briceño, Soporte, jbriceno@netactica.com

Juan Cruz Menéndez, Soporte de auditoria en Ciberseguridad, jmenendez@netatica.com

Cumplimiento de la norma PCI-DSS

En **NETACTICA** estamos en cumplimiento de la norma PCI-DSS (Payment Card Industry Data Security Standard) norma que aplica a cualquier compañía que procese, almacene o transmita datos de tarjeta de sus clientes.

La responsabilidad del cumplimiento de este estándar recae sobre todos los empleados de la compañía ya que los controles cubren todos los activos que componen una empresa:

Normas de seguridad de datos de la PCI: descripción general de alto nivel

Desarrolle y mantenga redes y sistemas seguros.	1. Instale y mantenga una configuración de *firewall* para proteger los datos del titular de la tarjeta. 2. No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta	3. Proteja los datos del titular de la tarjeta que fueron almacenados 4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	5. Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente. 6. Desarrollar y mantener sistemas y aplicaciones seguros
Implementar medidas sólidas de control de acceso	7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. 8. Identificar y autenticar el acceso a los componentes del sistema. 9. Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	10. Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta 11. Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	12. Mantener una política que aborde la seguridad de la información para todo el personal

El objetivo de esta norma es garantizar la seguridad de los datos de tarjeta de los clientes alrededor del mundo y su cumplimiento está ligado al manejo que se le dan a los datos dentro de las compañías. No cumplir con esta normatividad podría llevar a multas, fraudes e incumplimientos con nuestros clientes y aliados.

Políticas de Seguridad en la Red

Es fundamental que todo el personal que acceda o utilice los componentes de red de Netactica cumpla con las políticas establecidas en las Listas de Control de Acceso (ACL, por sus siglas en inglés). Para garantizar esto, es esencial que cada actor conozca, comprenda y acepte el contenido de este documento.

A continuación, se detallan las medidas de seguridad que deben ser implementadas:

1. Se debe configurar un ACL perimetral en cada conexión a Internet y entre cualquier Zona Desmilitarizada (DMZ).
2. Las reglas del firewall deben ser documentadas en un informe específico, el cual debe ser revisado y aprobado por las partes pertinentes.
3. Es necesario llevar a cabo una revisión semestral de las reglas del Firewall para garantizar que no se hayan realizado alteraciones no autorizadas. Este proceso debe quedar registrado utilizando el formato REQ 1- FOR 01: REVISIÓN SEMESTRAL DE REGLAS Y CONFIGURACIÓN DE FIREWALLS Y ELEMENTOS DE RED.
4. Se deben implementar configuraciones de anti-spoofing en el firewall.
5. Las redes deben ser segmentadas según su nivel de importancia y/o función.
6. Cualquier nueva regla o modificación en las existentes debe ser gestionada a través de un proceso de control de cambios.
7. El firewall debe contar con reglas que denieguen todo tráfico no autorizado, permitiendo únicamente aquel que esté definido en los puertos específicos.
8. El tráfico del firewall debe restringirse exclusivamente a lo necesario para las operaciones comerciales.
9. Los valores por defecto deben eliminarse de la configuración del firewall antes de implementarlo en el entorno de producción.
10. Todo tráfico no explícitamente permitido debe ser bloqueado o denegado por defecto.
11. Los diagramas de red y de flujo deben actualizarse cada vez que se realicen cambios en la configuración de la ACL.

Seguridad de Sistemas y Redes

En **NETACTICA**, mantenemos un enfoque sólido en la protección de nuestros sistemas y redes. Para lograrlo, hemos establecido las siguientes pautas y directrices:

- El software antivirus estándar aprobado por **NETACTICA** es Windows Defender. Este programa debe estar instalado y actualizado en todas las plataformas, incluyendo, pero no limitado a, Servidores de Archivos, Computadoras Personales y otros componentes críticos del sistema que sean compatibles.

- Es obligatorio implementar un software antivirus en todos los componentes que puedan estar vulnerables a software malicioso.
- Es vital que el antivirus se mantenga constantemente actualizado de manera automática para protegernos contra nuevas amenazas.
- Se requiere que los programas antivirus realicen análisis periódicos en cada componente donde estén instalados.
- Los antivirus deben generar registros de auditoría (logs) en los componentes donde estén activos, y estos registros deben ser conservados.
- Solo los usuarios con permisos de administración tienen la autorización para realizar cambios o desactivar la configuración de los programas antivirus.
- Es responsabilidad de cada usuario asegurarse de que sus equipos cuenten con los últimos parches de seguridad y el antivirus actualizado, tanto en computadoras personales como en servidores de red y otros dispositivos.
- Se prohíbe estrictamente el uso de dispositivos y medios de almacenamiento removibles en las estaciones de trabajo.
- El Oficial de Seguridad es responsable de mantener a los empleados informados acerca de los riesgos de infección por virus provenientes de correos electrónicos, sitios web y el intercambio de archivos. (Esta responsabilidad está vinculada a la capacitación del personal de **NETACTICA**).

Registro y Supervisión de Accesos a los Componentes del Sistema

En **NETACTICA**, tomamos en serio la seguridad y el control de acceso a nuestros sistemas. Las siguientes directrices y medidas garantizan una gestión efectiva de los registros y la supervisión de accesos:

Las bitácoras de auditorías se generan y almacenan por el período acordado para documentar las actividades de los usuarios, excepciones y eventos de seguridad de la información. Esto facilita investigaciones futuras y el monitoreo del control de acceso. Los controles incluyen:

- Todos los accesos deben ser registrados, y en caso de visualizar registros, es obligatorio dejar un rastro de dicha actividad en la aplicación donde se evidencia que existe un usuario propio por cada persona y queda registrado en los logs.
- todo acceso a las redes de **NETACTICA** debe ser monitoreado.
- Cualquier acceso a los registros por parte de administradores.
- Escalado de privilegios.
- Acceso a todos los registros.
- Creación, eliminación o modificación de usuarios en los componentes del sistema con permisos de administrador o root.
- Accesos concedidos y fallidos de usuarios.
- Inicialización, pausa o detención de la grabación de registros.
- Creación o eliminación de objetos del sistema.

Los registros de auditoría incluyen:

- Identificador de usuario específico.
- Fecha y hora.
- Tipo de evento.
- Componente afectado.
- Estado (erróneo o exitoso).
- Origen de la acción.

Además:

- Se implementan medidas técnicas, físicas y administrativas para asegurar la integridad y disponibilidad de los registros de auditoría. Se retienen los registros durante un año, con los últimos tres meses disponibles para su consulta.
- Todos los registros de auditoría deben centralizarse en un componente separado (Wazuh), evitando su almacenamiento local. .

- Se garantiza que los registros de auditoría de los componentes del sistema se recolecten de manera segura y no puedan ser alterados durante el almacenamiento.
- Los accesos a los registros por parte de los administradores también son registrados.
- Se lleva a cabo una revisión diaria de los registros y se toman acciones apropiadas frente a cualquier actividad no autorizada detectada.
- El acceso a los registros está limitado a empleados cuyo rol lo requiera; cualquier intento de acceso no autorizado será bloqueado.
- En casos de eventos con alta criticidad, se generan alertas para que los administradores tomen acción inmediata.
- Los registros almacenados no deben contener información confidencial de tarjetahabientes.
- Para asegurar un seguimiento adecuado de eventos, todos los sistemas deben sincronizarse con el servidor NTP interno.

Política de dispositivos portátiles.

- Únicamente a través de la VPN esta permitido que los funcionarios administradores de **NETACTICA** se conecten mediante dispositivos móviles a los servidores de la empresa.
- Todo dispositivo portátil que se conecte al CDE a las redes públicas e internet y sea de **NETACTICA**, personal del empleado o clientes, debe tener una configuración de firewall y antivirus o equivalente la cual debe estar ejecutándose activamente y de la misma forma es prohibido alterar las configuraciones realizadas en los firewall y antivirus de estos componentes.

Detección e informe oportuno de fallas.

Netactica debe detectar y responder ante fallas que se puedan presentar de:

- *WAF*
- IDS
- FIM (Wazuh)
- Antivirus (Deffender)
- Controles de acceso lógico
- Mecanismos de registro de auditoría (Wazuh)
- Controles de segmentación (Subnets AWS)

Los procesos para responder en caso de fallas en el control de seguridad son los siguientes:

- Restaurar las funciones de seguridad
- Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad
- Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la remediación requerida para abordar la causa raíz
- Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad
- Realizar una evaluación de riesgos para determinar si se requieren más acciones como resultado de la falla de seguridad
- Implementar controles para prevenir que se vuelva a producir la causa de la falla
- Reanudar la supervisión de los controles de seguridad

Uso interno Netactica:

- [ ] Certifico haber recibido, leído y comprendido el contenido del presente documento en su totalidad

Firma:

Aclaración:

Fecha: