REPÚBLICA DE GUATEMALA **EJÉRCITO DE GUATEMALA**

“II Curso Internacional de Informática y Ciberdefensa”

CURSO:

SEGURIDAD DE INFORMATICA II

TEMA:

POLITICAS DE CONTROL DE ACCESOS

ALUMNO

TTE. DE INF. MORALES BATZ

INSTRUCTOR

TTE. DE ART. ANIBAL LOPEZ MENDOZA

GUATEMALA, 18 DE SEPTIEMBRE DE 2023.

INTRODUCCIÓN

La siguiente política establece los criterios fundamentales para nuestra empresa, lo que ayudará a salvaguardar la integridad y seguridad de nuestros activos digitales y garantizar un entorno cibernético protegido.

OBJETIVO

El objetivo principal de esta política es garantizar un acceso seguro, autorizado y controlado a los equipos informáticos y sistemas de información de la empresa, a través de la implementación de esta política.

ALCANCE

El propósito de esta política es establecer pautas para garantizar el acceso seguro y autorizado a los equipos informáticos de la empresa de ciberseguridad.

Esta política se aplica a todos los empleados, contratistas y terceros que acceden a los sistemas y recursos informáticos de la empresa.

POLÍTICA

1. Se requerirá autenticación para acceder a los sistemas, utilizando credenciales únicas y seguras.
2. La autenticación multifactor (MFA) será obligatoria para cuentas con acceso a datos sensibles o sistemas críticos (TOKEN, VERIFICACION BIOMETRICA)
3. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
4. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.
5. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
6. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.
7. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
8. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.
9. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
10. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.
11. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
12. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.

13. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
14. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.
15. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
16. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.
17. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
18. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.
19. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
20. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.
21. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
22. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.
23. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
24. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.
25. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
26. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.
27. Los usuarios recibirán permisos y roles de acceso específicos basados en sus responsabilidades laborales.
28. La asignación de permisos se realizará de acuerdo con el principio de "menos privilegios", donde los usuarios solo tendrán acceso a los recursos necesarios para su trabajo.

CUMPLIMIENTO

A. Medidas de cumplimiento

    1. La administración de sistemas supervisará de manera constante el cambio de contraseñas para garantizar que se cumplan los plazos establecidos y que las contraseñas sean actualizadas según lo requerido por la política.

2. Se establecerán procedimientos de sanitización de archivos para garantizar la eliminación segura de datos confidenciales en dispositivos y sistemas antes de su reutilización o disposición final.

3. Se implementará un sistema de control de acceso basado en la clasificación de datos, donde los datos sensibles o confidenciales recibirán niveles más altos de seguridad y control de acceso.

4. Se proporcionará información regular sobre las actualizaciones y parches de seguridad disponibles, y se requerirá que los usuarios los apliquen de manera oportuna en sus sistemas.

5. Se establecerá un procedimiento claro para que los empleados reporten cualquier incidente de seguridad o posible violación de acceso. Esto permitirá una respuesta rápida y efectiva a las amenazas.

6. La empresa llevará a cabo auditorías internas y, si es necesario, externas, para evaluar el cumplimiento de esta política y la eficacia de las medidas de seguridad.

7. La política de control de acceso se mantendrá actualizada y se documentará de manera adecuada para garantizar su accesibilidad y comprensión por parte de todos los empleados.

8. Se realizarán evaluaciones periódicas de terceros y proveedores de servicios que tengan acceso a sistemas y datos de la empresa para garantizar que cumplan con los estándares de seguridad requeridos.

9. Se implementarán medidas de gestión de sesiones para garantizar que las sesiones inactivas se cierren automáticamente, reduciendo así el riesgo de acceso no autorizado debido a la inactividad o intento.

B. NO CUMPLIMIENTO

1. Sanciones Disciplinarias: Los empleados que no cumplan con esta política pueden estar sujetos a sanciones disciplinarias, que pueden variar desde una advertencia por escrito hasta la terminación del empleo, dependiendo de la gravedad del incumplimiento.

2. Revocación de Privilegios: En casos graves de no cumplimiento, se puede revocar el acceso a los sistemas y recursos digitales de la empresa, lo que podría afectar la capacidad del empleado para realizar sus funciones laborales.

3. Riesgo de Seguridad: El no cumplimiento puede aumentar el riesgo de violaciones de seguridad, pérdida de datos o acceso no autorizado a sistemas, lo que podría tener un impacto negativo en la empresa y sus clientes.

4. Responsabilidad Legal: En algunos casos, el no cumplimiento de políticas de seguridad cibernética puede tener implicaciones legales y resultar en responsabilidad civil o penal para el individuo y la empresa.

ESTÁNDARES Y POLÍTICAS RELACIONALES

1. Política de Terceros y Proveedores
2. Política de Gestión de Contratos de Seguridad.
3. Política de Comunicación de Incidentes con Terceros
4. Política de Cumplimiento Normativo para Terceros
5. Política de Evaluación de Riesgos de Terceros
6. Política de Auditoría y Revisión de Terceros

DEFINICIONES Y TÉRMINOS

1. Autenticación Multifactor (MFA): Método de seguridad que requiere que los usuarios proporcionen múltiples formas de identificación antes de permitir el acceso a sistemas o datos sensibles. Esto puede incluir credenciales, tokens o verificación biométrica.

2. Credenciales: Información de inicio de sesión, que generalmente consiste en un nombre de usuario y una contraseña, utilizada para verificar la identidad de un usuario antes de permitir el acceso a sistemas o recursos.

3. Principio de "Menos Privilegios": Un enfoque de seguridad que garantiza que los usuarios solo tengan acceso a los recursos y datos necesarios para llevar a cabo sus responsabilidades laborales. Se busca minimizar los riesgos reduciendo el acceso innecesario.

4. Datos Sensibles o Confidenciales: Información que, si se divulga o se accede de manera no autorizada, podría tener un impacto significativo en la empresa, sus clientes o sus socios. Esto incluye datos personales, financieros y de propiedad intelectual.

5. Supervisión de Cambio de Contraseñas: Proceso continuo de verificación del cumplimiento de los plazos establecidos para el cambio de contraseñas, asegurando que las contraseñas se actualicen según lo requerido por la política.

6. Sanitización de Archivos: Procedimiento de eliminación seguro de datos confidenciales en dispositivos y sistemas antes de su reutilización o disposición final, para prevenir la recuperación no autorizada de información.

7. Control de Acceso Basado en la Clasificación de Datos: Sistema que asigna niveles de seguridad y control de acceso en función de la clasificación de los datos, otorgando mayor protección a los datos sensibles o confidenciales.

8. Actualizaciones y Parches de Seguridad: Mejoras y correcciones de software diseñadas para abordar vulnerabilidades y mejorar la seguridad de los sistemas. Los usuarios deben aplicar estas actualizaciones de manera oportuna.

9. Reporte de Incidentes: Procedimiento claro y definido para que los empleados notifiquen cualquier incidente de seguridad o posible violación de acceso, permitiendo una respuesta efectiva a las amenazas.

10. Auditorías Internas y Externas: Evaluaciones sistemáticas de cumplimiento y seguridad, realizadas tanto por personal interno como por auditores externos, para evaluar el cumplimiento de la política y la eficacia de las medidas de seguridad.

11. Documentación de Política de Acceso: Registros y documentación que describen y mantienen la política de control de acceso de la empresa, asegurando su accesibilidad y comprensión por parte de los empleados.

12. Evaluación de Terceros: Proceso de revisión y evaluación periódica de terceros y proveedores de servicios que tienen acceso a sistemas y datos de la empresa para garantizar su cumplimiento con los estándares de seguridad requeridos.

13. Gestión de Sesiones: Medidas implementadas para supervisar y gestionar las sesiones de usuario, incluyendo la terminación automática de sesiones inactivas para reducir el riesgo de acceso no autorizado debido a la inactividad.