Políticas de ciberseguridad: Presidencia de la República

Autores:
Santiago Aillon Prada
Santiago Romero Lozano

Políticas aprobadas por:
Juan Carlos Bodoque

Ultima revisión:
20 de febrero de 2024

Revisión realizada por:
Santiago Aillon Prada
Santiago Romero Lozano

Tabla de contenidos

1 Introducción

La protección de la información es una prioridad absoluta para la Presidencia de la República de Colombia, tanto en el ámbito físico como en el digital. Reconocemos que la seguridad de los datos es fundamental para preservar los intereses del gobierno y proteger los activos críticos de la nación. Con el fin de evitar posibles impactos que puedan afectar o generar pérdidas para la organización y sus partes interesadas, implementamos políticas integrales de ciberseguridad, las cuales van a ser presentadas en el presente documento.

2 Clasificación de la información

2.1 Alcance

Esta política se aplica a todos los empleados, contratistas y terceros que manejan información en nombre de la Presidencia de la República.

2.2 Principios

Información Pública: Información que puede ser divulgada al público en general sin restricciones. Información Interna: Información que no está destinada al público en general, pero puede ser compartida dentro de la organización. Información Confidencial: Información que contiene datos sensibles y sólo puede ser accedida por personal autorizado. Información Secreta: Información que, si se divulga, podría causar daño grave a la seguridad nacional. Sólo personal con autorización especial puede acceder a esta información.

2.3 Objetivo

Esta política tiene como objetivo garantizar que toda la información manejada se clasifique de manera adecuada para proteger la seguridad nacional y los intereses del Estado.

2.4 Responsabilidades

- Todos los empleados deben clasificar la información que manejan de acuerdo con estas categorías.
- Los empleados deben manejar la información de acuerdo con su clasificación para evitar la divulgación no autorizada.

3 Control de acceso

3.1 Alcance

Protección de los activos de información de la organización a nivel físico, digital, aplicaciones y plataformas tecnológicas tanto en la red interna como las que interactúan con internet.

3.2 Principios

Preservar la Confidencialidad, Integridad y Disponibilidad de la información de la organización y de las partes interesadas que sea objeto de tratamiento, tanto en la red interna como las que interactúan con internet.

3.3 Objetivos

Los objetivos de la presente política están orientados a salvaguardar los activos de información en el entorno físico, de red local y los que se encuentran interconectados a través de internet.

1. Garantizar la protección de los activos de información sensibles del gobierno colombiano mediante la implementación de mecanismos de control de acceso eficaces.

2. Minimizar el riesgo de acceso no autorizado a los sistemas y datos gubernamentales, preservando la confidencialidad, integridad y disponibilidad de la información.

3. Establecer un marco normativo claro y coherente que regule y estandarice los procedimientos de control de acceso en todas las entidades gubernamentales.

4. Facilitar el acceso oportuno a los recursos de información necesarios para el desempeño eficiente de las funciones gubernamentales, manteniendo al mismo tiempo un nivel adecuado de seguridad.

3.4 Responsabilidades

Las responsabilidades en la organización, frente a la seguridad de la información y la ciberseguridad se encuentra jerárquicamente establecidas así:

- Alta dirección, revisa y aprueba de forma periódica la eficacia y aplicabilidad de la política de acuerdo con la dinámica del negocio.

- El CISO, revisa y evalúa la aplicación de procedimientos de seguridad de la información y controles de ciberseguridad para asegurar la adecuada ejecución de las políticas relacionadas.

Las responsabilidades en la organización, frente al incumplimiento de esta política se encuentra establecida así:

- En caso del incumplimiento de esta política por primera vez, alta dirección enviará una alerta junto con una amonestación de un salario mínimo vigente.
- En caso de reincidencia en el incumplimiento de esta política, se procederá con la terminación del empleo del individuo en cuestión.

Es importante tener encuentra que esta política esta sostenida por la ley 1581 de 2012:

- TÍTULO II, Artículo 4°, f
- TÍTULO IV, Artículo 8°, f

4 Protección de datos

4.1 Alcance

Esta política se aplica a todos los sistemas, redes y datos manejados por la Presidencia de la República.

4.2 Principios

- Confidencialidad: Los datos deben ser accesibles solo para aquellos con autorización adecuada.
- Integridad: La información debe mantenerse precisa y completa.
- Disponibilidad: Los datos deben estar disponibles cuando se necesiten.

4.3 Objetivos

- Proteger la información contra el acceso no autorizado.
- Asegurar la integridad de los datos.
- Proporcionar acceso a la información cuando se necesite.

4.4 Responsabilidades

- Gerencia de Ciberseguridad: Desarrollar, implementar y mantener la política de ciberseguridad.
- Empleados: Cumplir con la política de ciberseguridad.
- Departamento de TI: Proporcionar formación y soporte para la implementación de la política.

5 Protección contra malware

5.1 Alcance

- Protección de los activos de información de la organización a nivel físico, digital, aplicaciones y plataformas tecnológicas tanto en la red interna como las que interactúan con internet.
- Acción y efecto de garantizar que el acceso a la información pertinente.
- Acción y efecto de garantizar que los sistemas tanto físicos, como digitales operen de manera adecuada y eficiente.

5.2 Principios

Garantizar la Preservación de la Confidencialidad, Integridad y Disponibilidad de la información de la organización y de las partes interesadas que sea objeto de tratamiento, en todas las instancias afectadas, para mitigar el riesgo de infección por malware, tanto en la red interna como en las conexiones externas a internet.

5.3 Objetivos

Los objetivos de la presente política están orientados a salvaguardar y prevenir cualquier daño, manipulación o robo de los activos de información en la red local y los que se encuentran interconectados a través de internet.

1. Salvaguardar los sistemas físicos y digitales de la organización contra la infiltración y propagación de malware.
2. Minimizar la exposición de la información sensible y los activos de la organización a las amenazas de malware, preservando así la confidencialidad, integridad, disponibilidad y no repudio de la información.
3. Detectar y responder de manera rápida y oportuna a posibles incidentes de malware para limitar su impacto y prevenir la pérdida de datos o la interrupción de los servicios.
4. Establecer y mantener medidas de protección pro-activas, como el uso firewalls y la aplicación de políticas de seguridad robustas, para mitigar el riesgo de infección por malware.
5. Capacitar y concienciar al personal sobre las mejores prácticas de seguridad para prevenir la introducción y propagación de malware en los sistemas de la organización.

5.4 Responsabilidades

Las responsabilidades en la organización, frente a la seguridad de la información y a la protección contra el malware se encuentra jerárquicamente establecidas así:

- Alta dirección, revisa y aprueba de forma periódica la eficacia y aplicabilidad de la política de acuerdo con la dinámica del negocio.
- El CISO, revisa y evalúa la aplicación de procedimientos de seguridad de la información y controles de ciberseguridad para asegurar la adecuada ejecución de las políticas relacionadas.
- El CISO levará a cabo pruebas de penetración de forma semanal con el fin de garantizar la ausencia de vulnerabilidades en los sistemas y asegurar la integridad y seguridad de la infraestructura tecnológica.

Las responsabilidades en la organización, frente al incumplimiento de esta política se encuentra establecida así:

- En caso del incumplimiento de esta política por primera vez, alta dirección enviará una alerta junto con una amonestación de un salario mínimo vigente.
- En caso de reincidencia en el incumplimiento de esta política, se procederá con la terminación del empleo del individuo en cuestión.

Es importante tener encuentra que esta política esta sostenida por la ley 1581 de 2012 y la ISO 27001

6 Respuesta a incidentes

6.1 Alcance

Este plan se aplica a todos los incidentes de seguridad cibernética que afecten a los sistemas, redes y datos manejados por la Presidencia de la República. Esto incluye cualquier violación de la seguridad de la información que pueda tener un impacto significativo en las operaciones normales o en la privacidad de los empleados, clientes, socios o cualquier otra persona que haga negocios con la Presidencia de la República.

6.2 Principios

- Preparación: Anticiparse a los incidentes de seguridad mediante la formación de un equipo de respuesta a incidentes, la implementación de herramientas y procedimientos de seguridad, y la creación de un plan de comunicación.

- Detección: Identificar rápidamente los incidentes de seguridad mediante el monitoreo constante de los sistemas y la detección de actividades sospechosas.
- Respuesta: Actuar de manera rápida y eficaz ante un incidente de seguridad para minimizar el daño y la interrupción de las operaciones.
- Recuperación: Restaurar los sistemas a su estado normal de manera segura y eficiente después de un incidente.
- Aprendizaje: Aprender de cada incidente para mejorar la preparación y la respuesta en el futuro.

6.3 Objetivos

El objetivo de este plan es establecer un proceso eficaz y ordenado para responder a cualquier incidente de seguridad cibernética.

- Preparación: Esta fase implica la preparación para manejar posibles incidentes de ciberseguridad. Esto incluye la formación del equipo de respuesta a incidentes, la creación de un plan de comunicación y la implementación de herramientas y procedimientos de seguridad.
- Identificación: En esta fase, se identifica si ha ocurrido un incidente de seguridad. Esto puede implicar el monitoreo de los sistemas y la detección de actividades sospechosas.
- Contención: Una vez que se ha identificado un incidente, se deben tomar medidas para contenerlo y limitar el daño. Esto puede implicar la desconexión de sistemas afectados o la implementación de medidas de seguridad adicionales.
- Erradicación: En esta fase, se identifica la causa del incidente y se elimina. Esto puede implicar la eliminación de malware, la actualización de software o la modificación de los procedimientos de seguridad.
- Recuperación: Esta fase implica la restauración de los sistemas a su estado normal y la confirmación de que todos los sistemas están seguros antes de volver a la operación normal.
- Lecciones aprendidas: Después de un incidente, es importante revisar lo que ocurrió y aprender de él. Esto puede implicar la actualización del plan de respuesta a incidentes y la implementación de nuevas medidas de seguridad.

6.4 Responsabilidades

El equipo de respuesta a incidentes es responsable de llevar a cabo el plan de respuesta a incidentes. Todos los empleados son responsables de informar de cualquier actividad sospechosa y de seguir las políticas y procedimientos de seguridad.

7 Concienciación y formación de los empleados

7.1 Alcance

- Concienciación y formación de los empleados sobre las mejores prácticas de seguridad cibernética, con el objetivo de reducir el riesgo de incidentes de seguridad y así fortalecer la postura general de seguridad de la organización.
- Concienciación de los empelados respecto a las posibles consecuencias a nivel empresarial que pueden surgir si no se siguen estas prácticas.

7.2 Principios

Garantizar que los empleados tengan total conocimiento de la importancia de la preservación de la Confidencialidad, Integridad y Disponibilidad de la información de la organización y de las partes interesadas,

7.3 Objetivos

Los objetivos de la presente política están orientados a concientizar y educar a los empleados sobre practicas seguras que mitiguen o minimicen lo los incidentes de seguridad cibernética.

1. Elevar el nivel de conciencia y comprensión de los empleados sobre las amenazas y riesgos de seguridad cibernética que enfrenta la organización.
2. Fomentar una cultura de seguridad cibernética proactiva entre los empleados, promoviendo la adopción de comportamientos seguros y la participación activa en la protección de los activos de información.
3. Elevar el nivel de conciencia de los empleados sobre las posibles consecuencias de no llevar a cabo las practicas de seguridad cibernética.
4. Proporcionar formación continua y actualizada sobre las mejores prácticas de seguridad cibernética, herramientas y procedimientos pertinentes a las funciones laborales de los empleados.
5. Capacitar a los empleados para reconocer y reportar posibles incidentes de seguridad cibernética de manera oportuna y adecuada, contribuyendo así a una respuesta rápida y efectiva.

7.4 Responsabilidades

Las responsabilidades en la organización, frente a la seguridad de la información y a la protección contra el malware se encuentra jerárquicamente establecidas así:

- Alta dirección, revisa y aprueba de forma periódica la eficacia y aplicabilidad de la política de acuerdo con la dinámica del negocio.
- El CISO, realizara las diferentes charlas/cursos/cátedras mensualmente, enfocadas a concientizar e informar a los empelados sobre las diferentes practicas de seguridad cibernética.

Las responsabilidades en la organización, frente al incumplimiento de esta política se encuentra establecida así:

- En caso del incumplimiento de esta política por primera vez, alta dirección enviará una alerta junto con una amonestación de un salario mínimo vigente.
- En caso de reincidencia en el incumplimiento de esta política, se procederá con la terminación del empleo del individuo en cuestión.

Es importante tener encuentra que esta política esta sostenida por la ley 1581 de 2012 y la ISO 27001