POLÍTICA DE GESTIÓN DE INCIDENTES

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (PETI)
ARQUITECTURA EMPRESARIAL

Bogotá – Colombia
Noviembre de 2020

INDICE DE CONTENIDO

1. INTRODUCCIÓN

El presente documento define las directrices y lineamientos que colaboradores, contratistas o terceros deben tomar para gestionar el ciclo de vida de los Incidentes de Seguridad dentro de la Cámara de Representantes, desde el reconocimiento inicial del Incidente de Seguridad hasta el restablecimiento de las operaciones normales. Este proceso garantizará que todos los Incidentes de Seguridad sean detectados, analizados, contenidos y erradicados, que se tomen medidas para prevenir cualquier otro Incidente de Seguridad y, cuando sea necesario o apropiado, se notifique a las autoridades, al personal y/o a las partes interesadas, así como a la Alta Dirección.

2. OBJETIVOS

2.1. GENERAL

Establecer las pautas para asegurar que la Cámara de Representantes reaccione apropiadamente a cualquier incidente de seguridad real o potencial, relacionado con los sistemas de información y/o la información de la Entidad.

2.2. ESPECÍFICOS

- Definir el desarrollo de las capacidades de la Cámara de Representantes para responder rápida y eficazmente en caso de un incidente crítico.
- Implementar un enfoque integrado a la gestión de los riesgos asociados a los incidentes o a los incidentes críticos.
- Que se identifiquen y evalúen regularmente las amenazas y los posibles incidentes críticos a fin de reforzar la preparación de la Cámara de Representantes para esos acontecimientos.
- Garantizar que la Cámara de Representantes cuenta con procesos y procedimientos que faciliten la recuperación rápidamente de cualquier crisis y reanudar las operaciones normales lo antes posible.
- Definir los lineamientos para que todos Colaboradores, Contratistas, terceros y partes interesadas conozcan, apropien y apliquen esta política, así como la forma y los medios de cómo reportar un incidente.

3. ALCANCE Y ÁMBITO DE APLICACIÓN

La presente política tiene aplicabilidad a todos los sistemas de información que almacenan, procesan o transmiten datos de la Cámara de Representantes.

4. NORMATIVIDAD

NORMA	AÑO	DESCRIPCIÓN
NTC-ISO / IEC 27001:2013	2000	Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos
Ley 1273	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 734	2002	Código Disciplinario Único

5. DEFINICIONES Y TÉRMINOS

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas...) que tenga valor para la Entidad.

Activos de Información: Es todo aquello que contiene, procesa, trate y/o manipule información valiosa para la Entidad y que son necesarios para que la Entidad funcione y cumpla con los objetivos establecidos para dicho fin.

Autenticación: Es un proceso que garantiza y confirma la identidad de un usuario.

Análisis de Riesgo: Proceso que permite determinar cuán frecuentemente puede ocurrir eventos específicos y la magnitud de sus consecuencias.

La autenticación es uno de los aspectos básicos en la seguridad de la información, junto con los tres pilares, a saber: la integridad, disponibilidad, y confidencialidad.

CSIRT: Equipo o una entidad dentro de un organismo que ofrece servicios y soporte a un grupo en particular (comunidad objetivo) con la finalidad de prevenir, gestionar y responder a incidentes de seguridad de la información. Estos equipos suelen estar conformados por especialistas multidisciplinarios que actúan según procedimientos y políticas predefinidas, de manera que respondan, en forma rápida y efectiva, a incidentes de seguridad, además de coadyuvar a mitigar el riesgo de los ataques cibernéticos.

Comunicación: Intercambio de información entre dos o más usuarios a través de medios de transmisión alámbrico o inalámbricos por medio de señales eléctricas de tensión o corriente. El elemento que suministra la información se denomina emisor y el (los) que la(s) recibe(n) se denomina(n) receptor(es).

Evento: Una alerta o notificación creada por algún componente de la plataforma tecnológica de la información o herramienta de monitoreo.

Evento de Seguridad de la Información: Presencia identificada de una condición de un sistema, servicio o red, que indica que una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Evidencia digital: Información con valor probatorio almacenada o transmitida en forma digital.

Incidente: Es un evento o serie de eventos de seguridad de la información no deseado o no planeado, que afecte la prestación del servicio o reduzca la calidad de la prestación del servicio o que tenga una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información.

Incidente de Seguridad de la Información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y amenazar la seguridad de la información.

Log: Es un archivo en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

Monitoreo: Comprobar, supervisar, observar críticamente, o registrar el proceso de una actividad, acción o sistema en forma sistemática, para identificar cambios.

Restricciones: Por lo general las restricciones son establecidas o reconocidas por la dirección de la organización y están influidas por el entorno en el cual opera ésta**.**

Salvaguardar: Son prácticas, procedimientos o mecanismos que pueden proteger contra una amenaza, reducir una vulnerabilidad.

Solicitud del Servicio: Una solicitud de servicio es una petición de un usuario de información o asesoramiento, o de un cambio estándar, o para el acceso a un servicio de TI.

Vulnerabilidad: Muestra la fragilidad de un sistema (físico, Técnico, organizacional, cultural, etc.) que puede ser afectado adversamente, causando daños o perjuicios.

6. DESCRIPCIÓN DE LA POLÍTICA

La Cámara de Representantes debe implementar los mecanismos necesarios para el desarrollo de las capacidades para la gestión, identificación, detección, respuesta y recuperación frente a los incidentes de Seguridad de la Información y de Seguridad Digital.

La presente política debe aplicarse tan pronto como se sospeche que los sistemas de información o los datos están en funcionamiento, o están realmente afectados por un evento adverso que probablemente conduzca a un incidente de seguridad.

Un "Incidente de Seguridad en la Gestión de la Información" es un evento adverso que ha causado o tiene el potencial de causar daños a los bienes, la reputación y/o a colaboradores, contratistas y terceros de la Entidad. La gestión de incidentes se ocupa de la intrusión, el compromiso y el mal uso de la información y recursos de información, y la continuidad de los sistemas y procesos de información críticos. Puede enfocarse inicialmente a los servicios de tecnología, pero también se aplica a los registros en papel, las cartas y cualquier otra forma los datos se almacenan o procesan.

6.1. LINEAMIENTOS

- Se deben establecer responsabilidades y procedimientos para garantizar la gestión y respuesta a los Incidentes de Seguridad y Privacidad de la Información de forma rápida, eficaz y ordenada a los incidentes de seguridad.
- Se debe definir y conformar un Equipo de Respuesta a Incidentes – CSIRT el cual es un grupo interdisciplinario que asume la gestión de los incidentes cuando se determine que sea necesario.
- Los objetivos de la gestión de los Incidentes de Seguridad deben ser acordados con la Alta Dirección, y se debe asegurar que los responsables de la gestión de los Incidentes de Seguridad entiendan las prioridades de la Entidad para manejar los Incidentes de Seguridad.
- La Cámara de Representantes debe propender por la generación de las capacidades para la gestión y la respuesta de incidentes de seguridad y privacidad de la información de forma transversal.
- Los Incidentes de Seguridad deben ser notificados a través de los canales de gestión apropiados tan pronto como sea posible.
- Los colaboradores, contratistas y terceros que utilizan los sistemas y servicios de información de la Entidad deben informar sobre cualquier debilidad o vulnerabilidad de seguridad observada o sospechada en los sistemas o servicios.
- Los Eventos de Seguridad y Privacidad deben ser evaluados, y se debe decidir si deben ser clasificados como Incidentes de Seguridad o Privacidad.
- Los Incidentes de Seguridad y Privacidad deben ser respondidos de acuerdo con los procedimientos documentados de Respuesta a Incidentes.
- Minimizar el impacto adverso de los incidentes de seguridad y privacidad de la información mediante la aplicación de los controles adecuados.
- Contar con prácticas para la generación, análisis y consolidación de lecciones aprendidas de frente al proceso de gestión y respuesta a incidentes de seguridad y privacidad de la información.

- El conocimiento obtenido del análisis y la resolución de los incidentes de seguridad y privacidad debería utilizarse para reducir la probabilidad o el impacto de futuros incidentes.
- Se deben definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de la información que pueda servir como prueba o como evidencia digital.
- Se debe concientizar sobre la gestión de los incidentes de seguridad y privacidad de la información, temas tales como:
    - Los beneficios de un enfoque formal y coherente de la gestión de incidentes (personal y organizacional);
    - Cómo funciona el programa, expectativas;
    - Cómo reportar incidentes de seguridad y privacidad, a quién contactar;
    - Las limitaciones impuestas por los acuerdos de no divulgación.
- Los canales de comunicación deben establecerse con suficiente antelación a un incidente de seguridad o privacidad. Incluya a todas las partes necesarias en la comunicación pertinente:
    - Miembros del Equipo de Respuesta a Incidentes – CSIRT.
    - La Alta Dirección.
    - Personal de apoyo de la Cámara de Representantes.
    - En caso de que se produzca un incidente de seguridad o de privacidad, los propietarios de datos, Organismos de apoyo Gubernamentales y otras partes necesarias deben ser notificados en un plazo razonable y en cumplimiento de los requisitos aplicables.
    - Partes interesadas.
- En ningún momento se deben obstaculizar injustificadamente las investigaciones sobre los incidentes de seguridad o privacidad.
- Cualquier obstrucción de una investigación de un evento o incidente de seguridad o privacidad debe ser inmediatamente comunicada a la alta dirección para su resolución.
- La obstrucción de una investigación puede dar lugar a medidas disciplinarias, que pueden incluir el despido.
- Establecer los mecanismos que permitan cuantificar y monitorear los tipos, cantidades y costos de los incidentes de seguridad de la información.
- Establecer las métricas apropiadas para la gestión de los incidentes de seguridad y privacidad de la información.

7. RESPONSABLES

- **Responsable de Seguridad de la Información**: Velar por el cumplimiento de la presente política para garantizar el desarrollo continuo de las capacidades de la Cámara de Representantes para responder a los incidentes de seguridad de la información y seguridad digital.
- **Responsable de la Oficina de Planeación y Sistemas**: Definir los controles necesarios que garanticen la apropiada gestión y respuesta de los incidentes de seguridad de la información y seguridad digital durante todo su ciclo de vida.
- Los roles necesarios y responsables de responder a un Incidente de Seguridad o Privacidad conforman el CSIRT, los miembros principales serán los siguientes:
    - Oficial de Seguridad de la Información (Líder del CSIRT).
    - Jefe de la Oficina de Planeación y Sistemas (Backup del Líder del CSIRT).
    - El personal del equipo de seguridad.
    - El personal del equipo del área de Sistemas.
    - El propietario de la información.
- Otros grupos y/o colaboradores que pueden ser necesarios incluyen:
    - Liderazgo de alto nivel.
    - Oficina Jurídica.
    - Oficina de Personal.
    - Mesa de Ayuda.
    - Otro personal involucrado en el incidente de seguridad o privacidad o necesario para la resolución del Incidente:
        - Contratistas (según sea necesario).
        - Recursos de comunicaciones.

8. INCUMPLIMIENTO

El incumplimiento de la Política de Gestión de Incidentes de la Entidad podrá constituir falta disciplinaria y será sancionada en el marco del Código Disciplinario Único – Ley 734 de 2002.

9. REFERENCIAS

- Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de Seguridad y Privacidad de la Información – 2016.
- Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de Seguridad y Privacidad de la Información, *Guía para la Gestión y Clasificación de Incidentes de*

Seguridad de la Información - 2016.

- International Organization for Standardization, ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems.

10. CONTROL DE CAMBIOS

Nº VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	APROBADO POR
1	16/12/2021	• 19/10/2020 Creacion del Documento. • 06/11/2020 Ajuste de Formato.	Oficina de Planeación y Sistemas Ing. Elgar Castillo Rueda – Jefe OPS Revisión Técnica: Ing. Alejandro Muñoz Sandoval Ing. Sebastián Del Toro Montalvo Ing. Álvaro Carreño Ortiz Aprobación: Comité Institucional de Gestión y Desempeño 16/12/2021