PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

CAJA DE PREVISIÓN SOCIAL MUNICIPAL DE BUCARAMANGA

TABLA DE CONTENIDO

INTRODUCIÓN

Actualmente para las empresas públicas y privadas la información representa el activo más importante, por lo tanto la seguridad de la información se ha convertido en un aspecto fundamental. Los constantes avances en tecnología y la creciente interconexión de sistemas y dispositivos han dado lugar a un aumento significativo de los riesgos y amenazas para la integridad, confidencialidad y disponibilidad de la información.

Los incidentes de seguridad de la información, que pueden variar desde intentos de acceso no autorizado hasta ciberataques sofisticados, representan una amenaza latente para cualquier empresa u entidad pública. La capacidad de detectar, responder y recuperarse rápidamente de estos incidentes se ha vuelto crucial para garantizar la continuidad del negocio y salvaguardar la confianza de clientes y socios.

El presente documento, tiene como objetivo establecer una guía para abordar los incidentes de seguridad de la información de la Caja de Previsión Social Municipal de Bucaramanga. Este procedimiento se basa en las mejores prácticas y estándares reconocidos a nivel mundial, y ha sido diseñado para facilitar una respuesta eficiente y coordinada ante cualquier evento que ponga en peligro la seguridad de los activos de información.

JUSTIFICACIÓN

La gestión de incidentes de seguridad de la información es una disciplina esencial que permite a las organizaciones detectar, responder y recuperarse de manera eficiente ante eventos adversos que pongan en riesgo la confidencialidad, integridad y disponibilidad de los datos críticos. Afrontar estos incidentes de manera adecuada y oportuna minimiza el impacto negativo y los riesgos asociados, garantizando así la continuidad operativa y la reputación de la organización.

La justificación de este documento radica en la necesidad de contar con un enfoque sistemático y unificado para la gestión de incidentes de seguridad de la información dentro de la Caja de Previsión Social Municipal de Bucaramanga, buscando garantizar los siguientes aspectos:

- Mitigación de daños: La capacidad de responder rápidamente a incidentes de seguridad ayuda a limitar los daños potenciales causados por ciberataques, evitando la pérdida de datos sensibles o la interrupción significativa de las operaciones.

- Cumplimiento normativo y legal: La implementación de un procedimiento de gestión de incidentes ayuda a cumplir con los requisitos legales y normativos relacionados con la protección de la información y la notificación de brechas de seguridad, lo que protege a la organización de posibles sanciones y daños a su reputación.

- Mejora de la preparación y planificación: Este documento proporciona una base sólida para desarrollar planes de contingencia y de respuesta ante incidentes específicos, lo que aumenta la resiliencia de la organización frente a amenazas futuras.

- Conciencia de seguridad: Al tener un procedimiento de gestión de incidentes implementado, se fomenta una cultura de seguridad en toda la organización, lo que lleva a una mayor conciencia y responsabilidad de todos los miembros en la protección de la información.

Este procedimiento se apoya en las recomendaciones del Modelo de Seguridad y Privacidad de la información MSPI, modelo impulsado desde el Ministerio de Tecnologías de la información y las comunicaciones MINTIC

CLASIFICACIÓN DE INCIENTES DE SEGURIDAD DE LA INFORMACIÓN

1. **Incidentes de Acceso No Autorizado:**
   - Intentos fallidos de inicio de sesión.
   - Accesos no autorizados a sistemas, aplicaciones o datos.
   - Uso no autorizado de cuentas de usuario.

2. **Malware y Códigos Maliciosos:**
   - Infección por virus, gusanos, troyanos o ransomware.
   - Detección de software malicioso en sistemas y dispositivos.
   - Intentos de distribución o propagación de malware.

3. **Phishing y Ingeniería Social:**
   - Intentos de obtener información confidencial mediante técnicas de ingeniería social.
   - Recepción de correos electrónicos o enlaces fraudulentos que buscan el robo de credenciales.

4. **Pérdida o Robo de Dispositivos:**
   - Pérdida o robo de dispositivos móviles, laptops, unidades USB u otros medios de almacenamiento con datos sensibles.
   - Posible exposición de información confidencial.

5. **Ataques de Denegación de Servicio (DoS/DDoS):**
   - Intentos de sobrecargar los sistemas, aplicaciones o redes para evitar que sean accesibles para usuarios legítimos.
   - Interrupción de servicios críticos.

6. **Brechas de Seguridad y Fugas de Datos:**
   - Acceso no autorizado a bases de datos o repositorios de información sensible.
   - Divulgación no autorizada de datos confidenciales.

7. **Intrusiones y Compromisos de Red:**
   - Detección de actividad sospechosa o no autorizada en la red.
   - Compromisos de sistemas y dispositivos.

8. **Incidentes de Riesgo Físico:**
   - Acceso no autorizado a áreas restringidas o de alta seguridad.
   - Daños físicos a equipos de TI y sistemas.

9. **Errores y Fallos de Sistemas:**
   - Incidentes causados por errores humanos o fallos técnicos que afectan la seguridad de la información.
   - Acciones involuntarias que ponen en riesgo la integridad de los datos.

QUE HACER EN CASO DE REGISTRAR UN INCIDENTE QUE AFECTE LA SEGURIDAD DE LA INFORMACIÓN

En caso de presentarse un incidente de seguridad que ponga en peligro la integridad de la información institucional o registrar alguna amenaza persistenete, se recomienda realizar el respectivo reporte a través de los siguientes canales: - ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), reportar al correo electrónico: contacto@colcert.gov.co o al Teléfono: (+571) 2959897. - CSIRT Gobierno reportar al correo csirtgob@mintic.gov.co - Centro cibernético Policial reportar en la siguiente ruta: https://caivirtual.policia.gov.co/

En caso de presentar algún evento que afecte la seguridad de la información institucional tenga en cuenta los siguientes pasos:

1. Desconecte la red: Si hay evidencia que los equipos de cómputo estás siendo atacados o infectados por malware, se deben desconectar inmediatamente de cualquier red, ya sea Wi-Fi o cableada. Esto evitará que el incidente se propague a otros sistemas.

2. Notificación al equipo de seguridad: se debe comunicar de inmediato al equipo de seguridad de la información o al responsable designado para gestionar incidentes. Si no hay un equipo específico, comunique la situación al supervisor o jefe inmediato.

3. Documente el incidente: Tome nota de todos los detalles relevantes sobre el incidente, como el momento en que ocurrió, cómo se descubrió, qué actividad inusual se observó y cualquier otra información pertinente. Esta documentación será valiosa para el análisis posterior y la respuesta adecuada.

4. Preserve las pruebas: Si es posible, evite alterar o manipular cualquier evidencia relacionada con el incidente. Preservar las pruebas es esencial para una investigación posterior y puede ser útil para identificar la fuente y el alcance del ataque.

5. Cambio de contraseñas: Si hay evidencia que las cuentas de usuario de los sistemas de información institucionales pueden haber sido comprometidas, cambie todas las contraseñas de acceso de inmediato. Utilce contraseñas fuertes y diferentes para cada cuenta, en lo posible adicione un segundo factor de autenticación.

6. Escanee su sistema en busca de malware: Después de desconectar los dispositivos de la red, realice un escaneo completo en busca de malware o virus utilizando un software antivirus actualizado.

7. Actualice sus sistemas y aplicaciones: Asegusere de que todos los sistemas operativos y aplicaciones estén actualizados con los últimos parches de seguridad y sistemas de antivirus. Esto ayudará a cerrar posibles brechas de seguridad.

8. Restaure desde una copia de seguridad confiable: Si el incidente ha causado pérdida de datos, restaure la información desde una copia de seguridad confiable. Asegurese de que las copias de seguridad sean almacenadas de manera segura y estén protegidas contra acceso no autorizado

GLOSARIO

- Privacidad de la información: Es el derecho fundamental de los individuos para controlar y proteger la información personal que les concierne, evitando su acceso, uso o divulgación no autorizada.
- Seguridad de la información: Es el conjunto de medidas y controles implementados para proteger la confidencialidad, integridad y disponibilidad de la información contra amenazas internas y externas.
- Riesgo: Es la posibilidad de que una amenaza explote una vulnerabilidad y cause daños o pérdidas a los activos de información, así como a la reputación de la organización.
- Evaluación de riesgos: Proceso sistemático para identificar, analizar y evaluar los riesgos asociados con la privacidad y seguridad de la información, determinando su impacto y probabilidad.
- Tratamiento de riesgos: Acciones y medidas tomadas para mitigar, transferir o aceptar los riesgos identificados durante la evaluación, con el objetivo de reducir su impacto o probabilidad.
- Análisis de impacto en la privacidad (AIPD): Evaluación que permite identificar y valorar los posibles impactos que el procesamiento de información personal puede tener en los derechos y libertades de los individuos.
- Brecha de seguridad: Incidente en el que la confidencialidad, integridad o disponibilidad de la información se ve comprometida debido a una violación de seguridad.
- Incidente de privacidad: Cualquier evento o situación que pueda comprometer la confidencialidad, integridad o disponibilidad de información personal, ya sea accidental o intencionalmente.
- Política de privacidad: Documento que establece los principios, prácticas y procedimientos que una organización sigue para proteger la información personal y garantizar el cumplimiento de las leyes y regulaciones aplicables.

- Auditoría de seguridad: Proceso de revisión y evaluación sistemática de los controles y medidas de seguridad implementados para determinar su eficacia y cumplimiento con los estándares y políticas establecidos.
- Responsable de protección de datos (DPO): Es el encargado designado dentro de una organización para supervisar y garantizar el cumplimiento de las leyes y regulaciones de protección de datos, así como para asesorar en materia de privacidad y seguridad de la información.
- Política de seguridad de la información: Documento que establece las directrices, responsabilidades y procedimientos para proteger los activos de información de una organización, incluyendo políticas específicas para la gestión de riesgos de privacidad.
- Evaluación de impacto en la protección de datos (EIPD): Proceso que implica evaluar de manera sistemática y detallada los posibles efectos y riesgos que las operaciones de procesamiento de datos pueden tener sobre la privacidad de los individuos.
- Vulnerabilidad: Debilidad o fallo en los controles de seguridad que puede ser explotado por una amenaza, lo que puede resultar en una brecha de seguridad o acceso no autorizado a la información.
- Amenaza: Cualquier evento o acción que tiene el potencial de causar daño a la confidencialidad, integridad o disponibilidad de la información, como ataques cibernéticos, robo de datos o desastres naturales.
- Plan de continuidad del negocio: Conjunto de procedimientos y medidas diseñados para garantizar la continuidad de las operaciones críticas de una organización en caso de interrupciones graves, como desastres, incidentes de seguridad o fallas del sistema.
- Gestión de incidentes: Proceso para detectar, responder, mitigar y recuperarse de incidentes de seguridad o brechas de privacidad, con el fin de minimizar el impacto y restaurar la normalidad lo antes posible.
- Sensibilización en seguridad: Actividades educativas y de concientización dirigidas a los empleados para promover la comprensión de las políticas, procedimientos y mejores prácticas de seguridad de la información, y fomentar una cultura de seguridad en la organización.

- Control de acceso: Medidas y políticas implementadas para garantizar que solo las personas autorizadas tengan acceso a la información y los recursos necesarios para realizar sus funciones, evitando accesos no autorizados.
- Gobierno de la privacidad: Marco de gobernanza y gestión que abarca las políticas, procesos y controles para asegurar el manejo adecuado de la información personal, el cumplimiento normativo y la protección de los derechos de los individuos.