BANCO CHN

CRÉDITO HIPOTECARIO NACIONAL

Gestión de Incidentes de Ciberseguridad

Que es un Incidente de Ciberseguridad: Es cualquier evento que compromete la **integridad, confidencialidad o disponibilidad** de los activos de información (computadoras, bases de datos, datos de clientes, etc.) de El Crédito.

¿Qué tipos de incidentes de seguridad hay?

Infecciones de código malicioso: Los incidentes en sistemas, equipos de trabajo o dispositivos móviles suelen iniciarse a través de correo electrónico, páginas web comprometidas, SMS o redes sociales.

Intrusiones o intentos de intrusión: Los problemas de seguridad son aprovechados por los ataques usan partes de programas y vulneran credenciales para comprometer cuentas y aplicaciones, incluyendo servicios web, resultando en suplantación de identidad o distribución de malware.

Fallos de disponibilidad: Ocurren cuando los atacantes hacen que un sistema, servicio o red no esté disponible para sus usuarios. Por ejemplo, en la banca en línea, un atacante puede enviar muchas solicitudes al servidor del banco, sobrecargándolo y evitando que los clientes accedan a sus cuentas o realicen transacciones.

Fraude: Se realiza principalmente mediante la suplantación de entidades legítimas para obtener beneficios económicos o mediante ataques de phishing para obtener credenciales de acceso a medios de pago.

¿Que es un Plan Gestión de Incidentes Cibernéticos?

Un **Plan de Gestión de Incidentes Cibernéticos**, es un documento estratégico que establece e implementa políticas y procedimientos para gestionar efectivamente los incidentes cibernéticos. Este plan debe considerar como mínimo las funciones siguientes:

USI-POL-002 Política de Gestión de Incidentes Cibernéticos.

Pasos para Gestionar Incidentes de Ciberseguridad

Protección: Está vinculada a la aplicación de medidas para proteger los procesos y los activos de la organización.

a) Controles de seguridad para la adquisición.
b) Gestión de cambios en configuraciones.
c) Gestión de control y autorización de acceso.
d) Prueba y mantenimiento de copias de respaldo de información.
e) Cumplimiento de regulaciones
f) Proceso de eliminación de datos y destrucción de dispositivos.
g) Protección por medio de encriptación o cifrado de datos.
h) Protección y restricción del uso de medios extraíbles y de dispositivos móviles.
i) Documentación, implementación y revisión de los registros de auditoría de los activos.

Identificación: Está función está vinculada a la comprensión del contexto de El Crédito, de los activos que soportan los procesos críticos de las operaciones y los riesgos asociados, considerando lo siguiente:

a) Gestión de activos: Deberán ser identificados, documentados y gestionados en forma consistente, en relación con los objetivos y la estrategia de riesgo de El Crédito.

b) Evaluación**:** El Crédito deberá identificar, analizar, clasificar y documentar sus vulnerabilidades cibernéticas, ciberamenazas, ciberataques e incidentes cibernéticos.

Pasos para Gestionar Incidentes de Ciberseguridad

Detectar: Está vinculada a la definición y ejecución de las actividades dirigidas a la identificación temprana de los incidentes de seguridad, considerando como mínimo lo siguiente:

a) Monitoreo continuo de la seguridad: Activos, accesos, conexiones, acciones que realizan sus usuarios internos y externos, acciones de los proveedores externos de El Crédito, para detectar vulnerabilidades cibernéticas, ciberamenazas, ciberataques a través de la implementación del equipo de respuesta a incidentes.

b) Correlación de Eventos: Evaluar los diferentes elementos de red que estuvieron involucrados en un incidente.

c) Base de conocimiento: Mantener y utilizar una base de información de conocimiento para hacer referencia rápida durante el análisis de incidentes.

d) Apoyo Externo: Solicitar apoyo externo cuando un incidente rebase las capacidades del equipo y recursos existentes, por lo que se debe considerar , realizar alianzas estratégicas con otras entidades y/o equipos de respuesta nacionales o extraterritoriales.

Pasos para Gestionar Incidentes de Ciberseguridad

Respuesta: Está vinculada a la definición y ejecución de las actividades apropiadas para garantizar una respuesta oportuna, durante y después de un incidente cibernético, tales como:

a) Todos los usuarios deben participar en la protección de la información, siguiendo las políticas de seguridad y ciberseguridad de El Crédito.
b) Mecanismos de convocatoria e integración del equipo de respuestas a incidentes cibernéticos.
c) Mecanismos para analizar, documentar y darle seguimiento a los incidentes o alertas recibidas de fuentes internas y externas.
d) Metodología de evaluación del impacto del incidente cibernético para su clasificación y categorización.
e) Actividades de mitigación de incidentes cibernéticos y sus efectos, documentando las mismas.
f) Análisis forense digital de los incidentes cibernéticos, debiendo elaborarse un informe técnico de los resultados obtenidos.

Recuperación: Se deben establecer y mantener mecanismos para resistir, responder y recuperarse de un incidente cibernético, con el objeto de restaurar cualquier activo o servicios relacionados a este, de conformidad con lo establecido en el plan de recuperación ante desastres (DRP) y el Plan de Recuperación de Incidentes Cibernéticos, tales como:

a) Identificación de los equipos afectados.
b) Validación de los equipos que funcionan normalmente y si corresponde corregir vulnerabilidades.
c) Incluir acciones para restaurar sistemas a partir de copias de seguridad limpias.
d) Reemplazar archivos comprometidos con versiones limpias, instalar parches, cambiar contraseñas, y ajustar la seguridad de la red.
e) Llevar el registro de los activos e ir documentando las vulnerabilidades corregidas.

Recordemos que
la Seguridad de la Información y
Ciberseguridad es responsabilidad de Todos

Unidad Seguridad de la Información

BANCO CHN

CRÉDITO HIPOTECARIO NACIONAL