Manual de Procedimiento

MANUAL PLAN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN (COMPUTER SECURITY INCIDENT RESPONSE “CSIRP”)

MAN-APY-342

Fecha: 11/12/2024
Versión: 2.1

Uso interno

Contenido

PLAN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN (COMPUTER SECURITY INCIDENT RESPONSE "CSIRP")

MAN-APY-342

1. Control documental

1.1. Resumen

El presente documento define el alcance del plan de respuesta a incidentes de seguridad informática para el BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMÁ, OCCIDENTAL BANK BARBADOS.

1.2. Propiedades del documento

Tipo de información	Datos del documento
Título	Plan de respuesta a incidentes de seguridad informática y de la información
Versión del documento	1.8
Fecha de actualización	Agosto 10 de 2023
Elaborado por	Lina Maria Molina – Diego Fernando Rivera P. – Edgar Javier Vija Salinas
Revisores	Cesar Augusto Cristancho

PLAN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN (COMPUTER SECURITY INCIDENT RESPONSE "CSIRP")

MAN-APY-342

2. Introducción

Un "Plan de respuesta a incidentes de Seguridad Informática y de la Información ("Computer Security Incident Response Plan" CSIRP) es un enfoque definido y documentado para gestionar las comunicaciones frente a posibles amenazas a los sistemas informáticos y los datos que son procesados y almacenados en estos sistemas. El CSIRP define un plan para una organización, indicando quien(es) debe(n) responder, con lineamientos de autoridad y responsabilidad claramente definidos.

El propósito del CSIRP es proveer una respuesta coordinada ante los incidentes de seguridad. El CSIRP establece el grupo de respuesta como primera línea de defensa ante la ocurrencia de un incidente de seguridad.

2.1. Visión

Este plan de respuesta a incidentes de seguridad informática y de la información (CSIRP) ha sido constituido con el fin de proporcionar una gestión coordinada y dar una respuesta a incidentes de seguridad informática y de la información que se puedan producir dentro de la infraestructura de red del BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMÁ, OCCIDENTAL BANK BARBADOS. La protección de la información almacenada y procesada dentro de la infraestructura de red del BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMÁ, OCCIDENTAL BANK BARBADOS debe tener la más alta prioridad.

Este CSIRP garantizará una respuesta eficaz y oportuna para hacer frente a todos los incidentes de seguridad informática y de la información que se podrían llegar a producir.

El Equipo de Respuesta a Incidentes de Seguridad informática (CSIRT) del BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMÁ, OCCIDENTAL BANK BARBADOS proporcionará una respuesta eficaz y coordinada a los potenciales incidentes de seguridad informática y de la información con el fin de evitar la pérdida o la exposición de datos sensibles, accesos no autorizados, robo de información y cualquier evento que pueda ocasionar pérdidas y poner en riesgo la operación del Banco. 7

2.2. Alcance

Este plan de respuesta a incidentes de seguridad informática y de la información

(CSIRP) se aplica a todos los activos que conforman la infraestructura de red, sistemas y dispositivos gestionados y administrados por BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMÁ, OCCIDENTAL BANK BARBADOS y define las acciones y medidas de comunicación que se deben seguir en caso de la ocurrencia de un incidente

de seguridad informática y de la información".

2.3. Misión

El equipo de respuesta a incidentes de Seguridad Informática y de la Información - CSIRT del BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMÁ, OCCIDENTAL BANK BARBADOS será el punto central de coordinación y acción en respuesta a un incidente y proveerá lo siguiente:
Respuesta rápida a los incidentes de seguridad que afecten la infraestructura de red y los activos informáticos del BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMÁ, OCCIDENTAL BANK BARBAROS

- Proteger los activos informáticos del BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMÁ, OCCIDENTAL BANK BARBADOS y los datos confidenciales procesados y almacenados en dichos activos informáticos en caso de que ocurra un incidente.
- Minimizar la interrupción de los servicios informáticos de la red ofrecidos a los clientes internos y externos, así como a los socios de negocios, proveedores, terceros y la comunidad en general, en caso de que ocurra un incidente de seguridad.
- Minimizar el impacto financiero y reputacional frente a un incidente de seguridad informática para el BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMÁ, OCCIDENTAL BANK BARBADOS.

2.4. Definiciones

Evento – Un evento se define como una acción que ha ocurrido. Por ejemplo, Se sabe que alguien ha ingresado en su computador porque podemos ver al usuario acceder o ver las entradas del log que indican que una cuenta de usuario fue utilizada para acceder al sistema o podríamos ver indicadores de actividad después de que el usuario ha iniciado sesión (como actividad del navegador).

Incidente – Un incidente, o un "incidente de seguridad", pueden ser definido como cualquier violación implícita o explícita de las políticas de seguridad definidas.

Datos sensibles- Los datos sensibles son comúnmente definidos por los organismos reguladores como "Securities and Exchange Commission" (SEC) o "Payment Card Industry (PCI) Data Security Standards (DSS)" de Visa, o por la legislación específica regional. En general, "datos sensibles" son cualquier tipo de datos asociados con un individuo o individuos que, si llegan a ser expuestos, suponen un serio riesgo de robo de identidad, fraude, etc. Sin embargo, en muchas organizaciones, "datos sensibles" pueden también ser definidos como la propiedad intelectual (esquemas de diseño, fórmulas químicas, etc.).

Brecha - Deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma.
Intrusión - Acceso no autorizado a un sistema, dispositivo o infraestructura.

2.5. Categorías de incidentes

Un incidente de seguridad puede dividirse en una de las tres siguientes categorías, comúnmente conocido como la triada de la brecha o "Breach Triad".

- Infiltración
- Acceso a datos
- Ex filtración

Infiltración
La infiltración se refiere a los medios por los que el intruso obtuvo acceso a la red del BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMÁ, OCCIDENTAL BANK BARBADOS este acceso puede originarse interna o externamente y puede ser el resultado de una configuración incorrecta del sistema/servidor, una aplicación vulnerable y expuesta, controles de seguridad débiles o cualquier combinación de los anteriores.