



Procedure Manual

MANUAL INCIDENT RESPONSE PLAN CYBERSECURITY AND SECURITY OF THE COMPUTER SECURITY INCIDENT RESPONSE “CSIRP”)

MAN-APY-342

Date: 11/12/2024
Version: 2.1

Uso interno



Content

1. Document control.....	3
1.1. Summary.....	3
2.Introduction	4
2.1. Vision	4
2.2. Scope	5
2.3. Mission	5
2.4. Definitions	5
2.5. Incident Categories.....	6



CYBERSECURITY AND INFORMATION SECURITY INCIDENT RESPONSE (CSIRP) PLAN

MAN-APY-342

1. Document control

1.1. Summary

This document defines the scope of the incident response plan for computer security for BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMA, OCCIDENTAL BANK BARBADOS.

1.2. Propiedades del documento

Type of information	Document data
Title	Computer and Information Security Incident Response Plan
Document version	1.8
Date of update	August 10, 2023
Prepared by	Lina Maria Molina – Diego Fernando Rivera P. – Edgar Javier Vija Salinas
Reviewers	Cesar Augusto Cristancho



CYBERSECURITY AND INFORMATION SECURITY INCIDENT RESPONSE (CSIRP) PLAN

MAN-APY-342

1. Introduction

A "Computer and Information Security Incident Response Plan" ("Computer Security Incident Response Plan" CSIRP) is a defined and documented to manage communications against potential threats to systems computer science and the data that are processed and stored in these systems. The CSIRP defines a plan for an organization, indicating who should respond, with clearly defined guidelines of authority and responsibility.

The purpose of the CSIRP is to provide a coordinated response to incidents of safety. The CSIRP establishes the response group as the first line of defense against the occurrence of a security incident.

2.1. Vision

This computer and information security incident response plan (CSIRP) has been constituted in order to provide coordinated management and to give a Response to computer and information security incidents that may occur produce within the network infrastructure of the BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMA, OCCIDENTAL BANK BARBADOS. The protection of the information stored and processed within the network infrastructure of the BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMA, OCCIDENTAL BANK BARBADOS it should have the highest priority.

This CSIRP will ensure an effective and timely response to address all the Computer and information security incidents that could occur.

The Computer Security Incident Response Team (CSIRT) of the BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMA, OCCIDENTAL BANK BARBADOS provide an effective and coordinated response to potential incidents of IT and information security to prevent loss or exposure of sensitive data, unauthorized access, theft of information and any event that may cause losses and jeopardize the Bank's operations. 7





2.2. Scope

CYBERSECURITY AND INFORMATION SECURITY INCIDENT RESPONSE (CSIRP) PLAN

MAN-APY-342

This computer and information security incident response plan (CSIRP) applies to all assets that make up the network infrastructure, systems and devices managed and administered by BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMA, OCCIDENTAL BANK BARBADOS and defines the actions and Communication measures to be followed in the event of an incident of computer and information security".

2.3. Mission

The Computer and Information Security Incident Response Team - CSIRT of the BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMA, OCCIDENTAL BANK BARBADOS will be the central point of coordination and action in the response to an incident and provide the following:

Rapid response to security incidents affecting the network and computer assets of the BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMA, OCCIDENTAL BANK BARBAROS

- Protect the IT assets of the BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMA, OCCIDENTAL BANK BARBADOS and the data processed and stored on such IT assets in event of an incident.
- Minimize disruption to network computing services offered to internal and external customers, as well as business partners, suppliers, and the community at large, in the event of an incident of safety.
- Minimize the financial and reputational impact of a security incident
COMPUTER SCIENCE FOR BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMA, OCCIDENTAL BANK BARBADOS.

2.4. Definitions

Event – An event is defined as an action that has occurred. For example, It is known that someone has logged into their computer because we can see the user access or view log entries indicating that a user account was used to access the system or we might see activity indicators after the user You're signed in (as browser activity).



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

MAN-APY-342

Incident – An incident, or a "security incident," can be defined as any implicit or explicit violation of defined security policies.

Sensitive Data- Sensitive data is commonly defined by agencies reguladores como "Securities and Exchange Commission" (SEC) o "Payment Card Industry (PCI) Data Security Standards (DSS)" of Visa, or by specific legislation regional. In general, "sensitive data" is any type of data associated with a individual or individuals who, if exposed, pose a serious risk of theft of identity, fraud, etc. However, in many organizations, "sensitive data" can also be defined as intellectual property (design schemes, chemical formulas, etc.).

Breach - Deficiency of a computer or telematic resource that puts the information services or exposes the information itself.

Intrusion - Unauthorized access to a system, device, or infrastructure.

2.5. Incident categories

A security incident can be divided into one of the following three categories, commonly known as the Breach Triad.

- Infiltration
- Data Access
- Former leak

Infiltration

Infiltration refers to the means by which the intruder gained access to the network of the BANCO DE OCCIDENTE, BANCO DE OCCIDENTE PANAMA, OCCIDENTAL BANK BARBADOS this access may originate internally or externally and may be the result of incorrect system/server configuration, an application vulnerable and exposed, weak security controls, or any combination of the Previous.

