

2024

**Banco País**

15-6-2024

**Política de Respuesta ante Incidentes de Seguridad**

**Política de Respuesta ante Incidentes de Seguridad de Banco País**

**Versión 1.0.0**

**Estado:** ☒ Borrador en Trabajo ☐ Aprobado ☐ Adoptado

**Propietario del Documento:** Comité de Seguridad de la Información

**Última Fecha de Revisión:** Junio 2024

**Propósito**

El propósito de la Política de Respuesta ante Incidentes de Banco País es describir los requisitos para manejar los incidentes de seguridad de la información de manera eficaz y eficiente.

**Audiencia**

La Política de Respuesta ante Incidentes aplica a la alta dirección y a otros individuos responsables de proteger los Recursos de Información de Banco País.

**Contenido**

1. **Equipo de Manejo de Incidentes (EMI)**
2. **Equipo de Respuesta**
3. **Plan de Respuesta ante Incidentes (PRI)**
4. **Reporte de Incidentes**
5. **Notificación y Comunicación**
6. **Definiciones**
7. **Referencias**
8. **Excepciones**
9. **Aplicación**

**Política**

**Equipo de Manejo de Incidentes (EMI)**

* Se establecerá un Equipo de Manejo de Incidentes (EMI), compuesto por expertos legales, gerentes de riesgos y otros gerentes de departamento relevantes.
* El EMI es responsable de:
	+ Asegurar que las actividades de respuesta ante incidentes se realicen conforme a los requisitos legales, contractuales y regulatorios.
	+ Comunicaciones internas y externas relacionadas con incidentes de seguridad de la información.
	+ Asegurar que el personal esté capacitado en cómo reportar un posible incidente.

**Equipo de Respuesta**

* Se designará un Comandante de Respuesta ante Incidentes para supervisar y dirigir las actividades de respuesta de Banco País.
* El Comandante de Respuesta ante Incidentes formará y supervisará un Equipo de Respuesta ante Incidentes de Ciberseguridad (CSIRT).
* El CSIRT responderá a los incidentes de ciberseguridad identificados siguiendo el Plan de Respuesta ante Incidentes.
* El Comandante de Respuesta ante Incidentes es responsable de reportar adecuadamente los incidentes al CIO/EMI.

**Plan de Respuesta ante Incidentes (PRI)**

* El Comandante de Respuesta ante Incidentes es responsable de supervisar la creación, implementación y mantenimiento del Plan de Respuesta ante Incidentes.
* El Plan de Respuesta ante Incidentes debe ser aprobado por el CSIRT al menos una vez al año.

**Reporte de Incidentes**

* La gerencia debe proporcionar un medio para que todo el personal reporte posibles incidentes. Los métodos de reporte deben garantizar que un posible incidente se escale rápidamente a la persona adecuada.
* El departamento de IT es responsable de monitorear los registros de eventos, la gestión de vulnerabilidades y otros registros para actividades sospechosas.
* Todos los incidentes reportados deben ser evaluados por un miembro del CSIRT o EMI para determinar el tipo de amenaza y activar los procedimientos de respuesta apropiados. Todos los miembros del CSIRT o EMI deben estar familiarizados con cómo evaluar y escalar un posible incidente.
* El Comandante de Respuesta ante Incidentes debe reportar el incidente a la alta dirección.
* La alta dirección debe reportar cualquier posible brecha y/o incidentes que involucren datos de clientes al EMI prontamente.

**Notificación y Comunicación**

El EMI es responsable de asegurar que las notificaciones y comunicaciones, tanto internas como con terceros (clientes, proveedores, fuerzas del orden, etc.), se realicen de manera oportuna, de acuerdo con los requisitos legales, regulatorios y contractuales.

* **Personal:**
	+ El personal debe ser notificado siempre que un incidente o las actividades de respuesta ante incidentes puedan afectar sus actividades laborales.
	+ Las comunicaciones internas deben evitar el pánico, la difusión de información errónea y notificar al personal sobre los canales de comunicación apropiados.
* **Interacción con las Fuerzas del Orden:**
	+ La interacción con las fuerzas del orden y los servicios de emergencia debe ser coordinada por el Comandante de Respuesta ante Incidentes o un miembro del EMI.
	+ El asesor legal debe ser consultado en las comunicaciones con las fuerzas del orden.
* **Clientes y Socios:**
	+ Todos los clientes y socios afectados por el incidente deben ser notificados según el lenguaje contractual aplicable, los acuerdos de nivel de servicio (SLAs), los estatutos y/o regulaciones aplicables.
	+ Las comunicaciones con clientes y socios deben ser consistentes, con el mismo o similar mensaje entregado a cada uno.
* **Autoridades Regulatorias:**
	+ Solo los miembros del EMI tienen permitido discutir la naturaleza y/o los detalles de un incidente con cualquier agencia reguladora.
	+ El EMI debe contactar a los reguladores según sea requerido o tan pronto como sea práctico.
* **Medios Públicos:**
	+ El EMI o la alta dirección asignará un portavoz designado responsable de la comunicación con los medios.
	+ Las consultas de las agencias de medios deben ser dirigidas al portavoz designado y al EMI.

**Definiciones**

Ver Apéndice A: Definiciones

**Referencias**

* ISO 27002: 16
* NIST CSF: PR.IP, DE.DP, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS-IM, RC.CO
* Plan de Respuesta ante Incidentes
* Política de Gestión de Vulnerabilidades
* Estándar de Registro
* Estándar de Gestión de Vulnerabilidades

**Excepciones**

Se pueden solicitar excepciones a ciertas disposiciones de la política siguiendo el Proceso de Excepciones de Banco País.

**Aplicación**

El personal que viole esta política puede estar sujeto a acciones disciplinarias, que incluyen el despido y penas civiles o penales relacionadas. Cualquier proveedor, consultor o contratista que viole esta política puede estar sujeto a sanciones, incluyendo la eliminación de derechos de acceso, la terminación de contratos y penas civiles o penales relacionadas.

**Historial de Versiones**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versión** | **Fecha de Modificación** | **Fecha de Aprobación** | **Aprobado por** | **Razón/Comentarios** |
| 1.0.0 | Junio 2024 | Por definir | Comité de Seguridad de la Información | Origen del Documento |

**CONTACTO**

Para emergencias de seguridad o cotizaciones sobre servicios, comuníquese con nosotros en:

**Teléfono:** (829-246-0000) Ext. 767 – 1891

**Dirección:** Av. Winston Churchill &, Santo Domingo 10130

**Sitio Web:** bancopais.com/contacto