intiza

# Norma de Gestión de Incidentes de Seguridad

*Versión: 2.1*

| Confeccionó | Revisó | Aprobó |
|---|---|---|
| **BDO**<br>**Consultoría Externa** |  <br>**Carla Leiva - CISO** |  <br>**Francisco Canale - Director** |

# Contenido

## 1. Objetivo

Establecer las medidas y acciones necesarias que le permitirán a INTIZA actuar de manera eficiente y efectiva a la hora de detectar y gestionar un incidente de seguridad de la información.

## 2. Alcance

Esta norma involucra desde la detección de un evento de seguridad, el registro, la resolución, la verificación y comunicación y cierre de los mismos.

## 3. Responsabilidades

**Cualquier persona**, interna o externa a INTIZA, que detecte un incidente de seguridad, es responsable de:

- Informar el incidente detectado al área de Seguridad de Información.
- Reportar cualquier potencial o actual comportamiento anormal, debilidad, incidente o amenaza a los sistemas de información de la empresa.
- Comprender las pautas expuestas en esta norma y proceder de acuerdo con ellas.

**Seguridad de la Información** es responsable de:

- Determinar si el incidente se debió a una falla técnica o no.
- En caso de descarte de fallas técnicas, informar el incidente.
- Evaluar la necesidad de involucrar a personal externo o a autoridades oficiales ante la aparición de un incidente de seguridad.
- Analizar los reportes de fallas posibles en los sistemas y tomar la acción correspondiente.

- Realizar una investigación post-incidente para evaluar la posibilidad de eliminar o minimizar una ocurrencia similar en el futuro.
- Mantener una base de datos de incidentes para agilizar la resolución de futuras ocurrencias similares.

**Tecnología** es responsable de:

- Informar a Seguridad de la Información al momento de detectar un incidente de seguridad.
- Registrar los incidentes reportados.
- Categorizar y otorgar un nivel de criticidad a los incidentes para definir su prioridad e impacto y agilizar su solución.
- Resolver los incidentes que involucran a la infraestructura y tecnología de información.

## 4. Desarrollo

### 4.1. Gestión de Incidentes

La gestión de incidentes involucra, en términos generales, los siguientes pasos:

- Detección
- Registro
- Resolución
- Verificación
- Comunicación/Cierre

A continuación, se detallan las principales consideraciones a tener en cuenta por INTIZA a la hora de realizar la gestión de un incidente de seguridad:

#### 4.1.1. Detección

Cualquier persona que detecte un evento que se sospeche que pueda dañar el funcionamiento de la organización, debe comunicar el evento al responsable de Seguridad de la Información a través de las vías correspondientes.

#### 4.1.2. Registro

Realizar un registro del evento detectado detallando toda la información respecto al mismo, generando un ticket en la herramienta interna para tal fin. El ticket debe hacer referencia a incidentes de seguridad, e incluir los siguientes datos:

- Origen del problema.
- Fecha y hora del incidente.
- Dirección IP / Nombre DNS de los recursos comprometidos.
- Nombre / identificación del sistema, plataforma o aplicación afectada
- Descripción del incidente. Dicho punto, solo será requerido cuando el incidente sea de carácter “Crítico” para la INTIZA.

#### 4.1.3. Resolución

Ante un incidente de seguridad, el área de Seguridad de la Información de INTIZA deberá:

- Realizar el análisis de la información correspondiente al incidente.
- Determinar si el evento detectado es un incidente de seguridad y clasificarlo como tal para su tratamiento.
- Identificar todas las partes interesadas/afectadas y poner en conocimiento de las mismas la ocurrencia del incidente detectado.
- Realizar la resolución del incidente siguiendo las pautas a continuación:

#### 4.1.3.1. Búsqueda de Información y Seguimiento

Para poder ejecutar el seguimiento del incidente detectado, el área de Seguridad de la Información de INTIZA deberá:

- Mantener toda la información recopilada como confidencial.
- Detectar equipos o sistemas afectados / comprometidos.
- Recopilar toda la evidencia e información relacionada con los sistemas y / o recursos informáticos involucrados en el incidente de seguridad. Preservar la evidencia encontrada, evitando su destrucción.
- Analizar los sistemas afectados para determinar el origen del ataque, el propietario del activo y la dirección IP donde se originó el ataque.

#### 4.1.3.2. Neutralización

Una vez realizado el análisis del incidente, Seguridad de la Información de INTIZA deberá:

- Coordinar todas las acciones necesarias para acceder a dispositivos y / o aplicaciones, y proceder a neutralizar las acciones de ataque o intrusión.

#### 4.1.3.3. Investigación del incidente

Mitigado el incidente de seguridad, Seguridad de la Información de INTIZA deberá:

- Analizar toda la información para determinar el alcance del incidente.
- Correlacionar eventos haciendo una línea de tiempo.
- Establecer el nivel de compromiso alcanzado.
- Identificar las fallas de seguridad que llevaron al incidente.
- Registrar y documentar todas las acciones tomadas.
- Además, la documentación debe contener al menos la siguiente información:
    - Datos personales del investigador.
    - Tipo de incidente investigado.

- Evidencia analizada.
- Herramientas utilizadas.
- Evidencia obtenida.
- Procedimiento de análisis.
- Cronología y descripción del incidente

#### 4.1.3.4. Resolución del incidente

Una vez analizada la información de detalle del incidente, se realizan las acciones necesarias para dar resolución al problema que ocasionó el incidente, en conjunto con las áreas involucradas y eventualmente, de ser necesario con algún proveedor de servicios requerido.

### 4.1.4. Verificación

Seguridad de la Información verificará si el incidente está resuelto correctamente.

### 4.1.5. Comunicación y Cierre

Por último, Seguridad de la Información deberá:

- Registrar el incidente, reflejando la información del acontecimiento.
- Mantener un registro de los incidentes ocurridos con toda la información relevante, los pasos de análisis y resolución. Esta información puede usarse en el futuro para proporcionar un tratamiento similar a otros incidentes relacionados de manera más eficiente o para realizar análisis de tendencias y detectar posibles fallas en la configuración de seguridad de los sistemas.
- Mantener el nivel de acceso a incidentes para garantizar que solo el personal autorizado pueda acceder a ellos.
- Informar la resolución del incidente a las áreas involucradas.

La gestión y confección de un informe completo y detallado sobre el incidente ocurrido, solo será necesario para todos aquellos incidentes de carácter "Crítico" para INTIZA.

### 4.2. Clasificación de Incidentes de Seguridad

Los incidentes de seguridad deberán ser clasificados por el área de Seguridad de la Información según la siguiente categorización:

| CLASIFICACIÓN | | |
|---|---|---|
| **Clasificación** | **Tipo de incidente** | **Descripción y ejemplos prácticos** |
| **Contenido abusivo** | **Spam** | Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo. |
| | **Delito abusivo** | Contenido difamatorio o discriminatorio. Ej: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos. |
| | **Pornografía infantil, contenido sexual o violento inadecuado** | Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc. |
| **Contenido dañino** | **Sistema infectado** | Sistema infectado con malware. Ej: Sistema, computadora o teléfono móvil infectado con un rootkit. |
| | **Distribución de malware** | Recurso usado para la distribución de malware. Ej: recurso de una organización empleado para distribuir malware. |

| | | |
|---|---|---|
| **Obtención de información** | **Escaneo de redes (scanning)** | Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos. |
| | **Análisis de paquetes (sniffing)** | Observación y grabación del tráfico de redes. |
| | **Ingeniería social** | Recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, amenazas. |
| **Intento de intrusión** | **Explotación de vulnerabilidades conocidas** | Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades. Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS). |
| | **Intento de acceso con vulneración de credenciales** | Múltiples intentos de vulnerar credenciales. Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta. |
| | **Ataque desconocido** | Ataque empleando exploit desconocido. |
| **Intrusión** | **Compromiso de cuenta con privilegios** | Compromiso de un sistema en el que el atacante ha adquirido privilegios. |

| | | |
|---|---|---|
| | **Compromiso de cuenta sin privilegios** | Compromiso de un sistema empleando cuentas sin privilegios. |
| | **Compromiso de aplicaciones** | Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej: inyección SQL. |
| | **Robo** | Intrusión física. Ej: acceso no autorizado a las oficinas de INTIZA.. |
| **Disponibilidad** | **DoS (Denegación de servicio)** | Ataque de denegación de servicio. Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio. |
| | **DDoS (Denegación distribuida de servicio)** | Ataque de denegación distribuida de servicio. Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP. |
| | **Mala configuración** | Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto |
| | **Sabotaje** | Sabotaje físico. Ej: cortes de cableados de equipos o incendios provocados. |
| | **Interrupciones** | Interrupciones por causas ajenas. Ej: desastre natural. |
| | **Acceso no autorizado a información** | Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos. |

| | | |
|---|---|---|
| **Compromiso de la información** | **Modificación no autorizada de información** | Modificación no autorizada de información. Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware. |
| | **Pérdida de datos** | Pérdida de información Ej: pérdida por fallo de disco duro o robo físico. |
| **Fraude** | **Uso no autorizado de recursos** | Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales. |
| | **Derechos de autor** | Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez. |
| | **Suplantación** | Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos. |
| | **Phishing** | Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas o realice acciones que generen beneficio al delincuente. |
| **Vulnerable** | **Criptografía débil** | Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: servidores web susceptibles de ataques POODLE/FREAK. |
| | **Amplificador DDoS** | Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej: DNS open-resolvers o Servidores NTP con monitorización monlist. |
| | **Servicios con acceso potencial no deseado** | Ej: Telnet, RDP o VNC. |

| | | |
|---|---|---|
| | **Revelación de información** | Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis. |
| | **Sistema vulnerable** | Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema. |
| **Otros** | **Otros** | Todo aquel incidente que no tenga cabida en ninguna categoría anterior. |
| | **APT** | Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos. |

## 4.3. Taxonomía de Incidentes de Seguridad

Una vez que un incidente ha sido reportado debe ser evaluado para determinar si:

- Puede ser considerado como un incidente local o un incidente de toda la empresa.
- Requiere seguimiento y gestión por parte del responsable de Seguridad de la Información.

Existen una serie de factores que deben tenerse en cuenta al evaluar y dar prioridad a un incidente:

- ¿Cuándo y dónde ocurrió el incidente?
- ¿Cuál fue la causa del incidente?

- ¿Qué sistemas, aplicaciones y datos se ven afectados por el incidente?
- ¿Existen sistemas adicionales, aplicaciones o datos que puedan ser afectados?
- ¿Podría haber implicaciones legales o reglamentarias a partir de los incidentes?
- ¿Cuántos usuarios se ven afectados por el incidente?
- ¿Existen terceras partes implicadas en el incidente?
- ¿Alguna información respecto del incidente fue comunicado a terceros/externos?

Los incidentes deben ser priorizados en función de su impacto real o potencial de la Compañía, incluidas las consideraciones legales o reglamentarias.

A continuación, se define la forma de calcularlos y obtener un nivel de criticidad global para cada incidente:

| Criticidad de incidentes | Criticidad de los recursos afectados | | |
|---|---|---|---|
| Efectos negativos producidos por el incidente o potenciales | 1-Alto | 2-Medio | 3-Bajo |
| 1-Grave | Muy Grave | Grave | Moderado |
| 2-Moderado | Grave | Moderado | Leve |
| 3-Leve | Moderado | Leve | Leve |

A continuación, se detalla el criterio definido para la determinación de la criticidad ante la aparición de incidentes de seguridad:

| Criticidad del incidente | Definición | Tiempo de Respuesta |
|---|---|---|
| Muy Grave | Una caída importante de servicios de TI hacia usuarios finales; por ejemplo, un sistema crítico de negocios no se encuentra disponible, o está funcionando a un nivel mucho más reducido. | Inmediato (menos de 6 horas) |
| Grave | Caída de servicio mediante el cual los usuarios finales pueden acceder a algunos recursos de los sistemas, pero que seriamente impactan en las normales operaciones comerciales, la realización de trabajos en ambientes productivos y los impactos de un grupo de personas o persona que ejerza una función crítica para el negocio. | 24 horas |
| Moderado | Pérdida de servicio que posee un impacto moderado en las operaciones comerciales. | 48 horas |
| Leve | Pérdida de servicio que posee un bajo impacto en las operaciones comerciales y no inhibe de manera significativa la productividad | 10 días |

## 5. Referencias

### 5.1. Normativa Relacionada

| Categoría | Título | Código |
|---|---|---|

| | | |
|---|---|---|
| **Normativa Interna** | Política de Seguridad de la Información | PO-SI-01 |
| **Procedimiento** | Procedimiento de Gestión de Incidentes de Seguridad | PR-SI-17 |
| **Procedimiento** | Gestión de Servicios de TI | PR-TI-03 |

## 5.2. Definiciones

| Término | Descripción |
|---|---|
| **Incidente de Seguridad** | Consiste en la materialización de un riesgo, es decir, es la ocurrencia de una amenaza, que, aprovechando una Vulnerabilidad en el sistema de controles de seguridad, afecta alguna de las dimensiones de la seguridad de la información: confidencialidad, integridad y/o disponibilidad de un activo tecnológico de INTIZA. |
| **Gestión de Incidentes** | Es el conjunto de acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de la Entidad. Minimizando su impacto en el negocio y la probabilidad de que se repita. |
| **Amenaza** | Factor que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. |

| | |
|---|---|
| **Vulnerabilidad** | Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. |
| **Rootkit** | Un rootkit es un tipo de software malicioso diseñado para darle a un hacker la capacidad de introducirse en un dispositivo y hacerse con el control del mismo. Por lo general, los rootkits afectan el software o el sistema operativo del dispositivo que infectan, pero algunos pueden actuar sobre su hardware o firmware. |
| **Exploit** | Un exploit es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico. Estos comportamientos incluyen, por lo general, la toma del control de un sistema, la concesión de privilegios de administrador al intruso o el lanzamiento de un ataque de denegación de servicio (DoS o DDoS). |
| **Ataques POODLE** | El ataque POODLE (lo cual significa "Padding Oracle On Downgraded Legacy Encryption") es un “exploit” del tipo "ataque de intermediario" (MITM) que permite a un intruso, descifrar contenido selectivo dentro de la sesión SSL. |

| | |
|---|---|
| **Ataques FREAK** | Es una grave vulnerabilidad en algunos de los protocolos de cifrado de las comunicaciones más extendidos. La técnica de esta vulnerabilidad consiste en interceptar la comunicación entre cliente y servidor y forzar el uso de un cifrado vulnerable (lo que se conoce como hacer un downgrade). De esta forma, se estaría usando una clave RSA de 512 bits de longitud, algo que puede romperse con unas pocas horas y el hardware adecuado (que no es precisamente caro). |

## 6. Historial de Versiones

| Versión | Fecha | Resumen de Cambios |
|---|---|---|
| 1.0 | 01/11/2021 | Creación de la Norma de Gestión de Incidentes. |
| 1.0 | 27/01/2022 | Aprobado por Comité de Dirección: MI-DI-02- Minuta de Comité de Dirección N° 2. |
| 2.0 | 06/06/2022 | Modificación texto agregando mayor detalle de etapas de la gestión de incidentes de seguridad y categorías de clasificación y ajuste del nombre de la norma a “Gestión de Incidentes de Seguridad”. |
| 2.1 | 22/08/2024 | Modificación de encabezado y pie de página, se agregó tiempos de respuesta de acuerdo con la criticidad del incidente. |