# **OLX – Gestión de Incidentes**

# **Borrador**

**TABLA DE CONTENIDOS**

[OLX – Gestión de Incidentes 1](#_Toc387848993)

[Borrador 1](#_Toc387848994)

[1. Objetivo del Documento 2](#_Toc387848995)

[1.1. Alcance 2](#_Toc387848996)

[1.2. Misión 2](#_Toc387848997)

[2. Roles y Responsabilidades 2](#_Toc387848998)

[2.1. Gestor de Incidentes 3](#_Toc387848999)

[2.2. Coordinador de Incidentes 3](#_Toc387849000)

[2.3. Soporte de 1er Nivel (nivel Inicial) 3](#_Toc387849001)

[2.4. Soporte 2do Nivel (niveles Superiores) 3](#_Toc387849002)

[3. Proceso de gestión de incidentes 4](#_Toc387849003)

[3.1. Entradas, salidas y disparadores 4](#_Toc387849004)

[4. Diagrama del proceso 5](#_Toc387849005)

[5. Registro de Incidentes 5](#_Toc387849006)

[6. Prioridad, urgencia e impacto 6](#_Toc387849007)

[6.1. Definición de niveles de severidad 7](#_Toc387849008)

[7. Estados de los incidentes 8](#_Toc387849009)

[8. RIO (reunión de incidentes operativos) 8](#_Toc387849010)

[9. Control y mejora continua 9](#_Toc387849011)

[9.1. Métricas: 9](#_Toc387849012)

**INFORMACIÓN DEL DOCUMENTO**

**IDENTIFICACIÓN**

# Objetivo del Documento

Establecer los lineamientos generales de la Gestión de Incidentes, en búsqueda de resolver cualquier situación que cause una degradación o interrupción en los servicios brindados por OLX

## Alcance

Se establece como alcance inicial, los incidentes derivados del monitoreo y detección del equipo de infraestructura

## Misión

Restaurar la operación normal de los Servicios, tan rápido como sea posible y minimizar el impacto adverso a las operaciones de Negocio, asegurando así que se mantenga el mejor nivel posible de calidad de servicio y disponibilidad, poniendo énfasis en los servicios críticos.

# Roles y Responsabilidades

Para OLX se proponen los siguientes roles para la Gestión de Incidentes:

* Gestor de Incidentes
* Coordinador de Incidentes
* Soporte de 1° (Nivel inicial)
* Soporte de 2° (Niveles superiores)

## Gestor de Incidentes

Asegurar que se cumpla el Proceso de Incidentes, coordinar todas las tareas para lograr una resolución rápida de Incidentes de TI y asegurar el cumplimiento de los SLA mediante escalamientos.

Velar por el cumplimiento y mejora continua del proceso de Gestión de Incidentes y los niveles de servicio comprometidos.

## Coordinador de Incidentes

El rol de Coordinador de incidentes deberá distribuirse para cada servicio, inicialmente coincide con el responsable de cada servicio. Será notificado ante cada incidente y participará de decisión ante la resolución de los mismos.

Monitorea las incidencias de uno o varios servicios, escala al gestor de incidentes situaciones que se escapen de los tiempos establecidos.

Coopera en la detección y registro de incidentes, su resolución escalado y posible derivación. Puede modificar prioridad, urgencia o impacto de la incidencia en base a su conocimiento.

## Soporte de 1er Nivel (nivel Inicial)

El objetivo principal de este rol es el de proveer soluciones rápidas y efectivas en aquellos casos que sea posible o bien asegurar el escalamiento al área o persona de 2do Nivel adecuadas para la resolución del mismo.

Registrar, clasificar y dar un primer nivel de soporte de Incidentes. Escalar los Incidentes que no pueda resolver e informar e interactuar con el Coordinador de Incidentes.

## Soporte 2do Nivel (niveles Superiores)

Recibe y gestiona solicitudes de soporte técnico según los procedimientos acordados. A este nivel se derivan los incidentes que soporte de 1er nivel no puede resolver por estar más allá de su alcance. Clasifica, analiza y resuelve los incidentes que le son derivados. (Desarrollo, PLC, Proveedores, etc)

Ejecuta las actividades de investigar, diagnosticar y resolver Incidentes. Cuenta con conocimiento en un dominio específico.

# Proceso de gestión de incidentes

## Entradas, salidas y disparadores



#### Entradas:

* Registro de los detalles básicos del incidente.
* Información de la CMDB.
* Información sobre los cambios/release generados para resolver incidencias

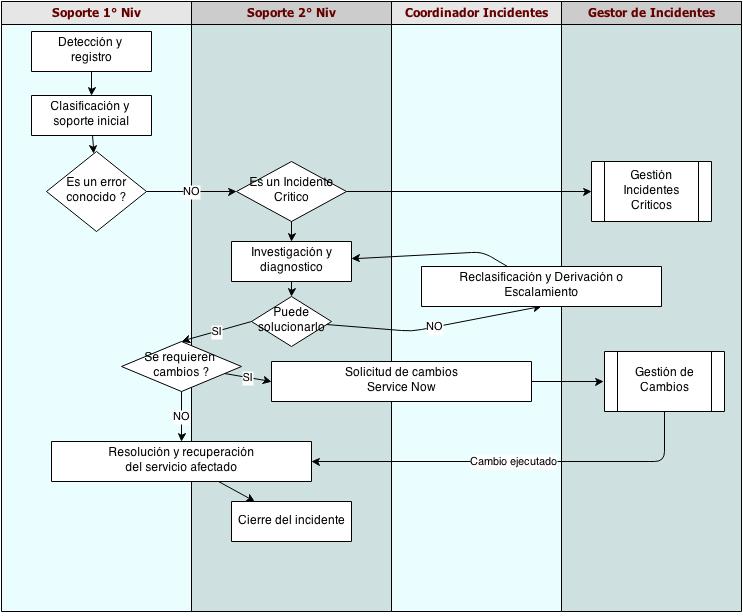
#### Salidas:

* Detalles del Incidente en curso
* Registro final del Incidente cerrado
* Generación de cambios para la resolución del incidente.

#### Disparadores:

* Llamada o mail reportando una incidencia.
* Alarma de Monitoreo
* Alarma de aplicaciones
* SLA incumplidos

# Diagrama del proceso



# Registro de Incidentes

Campos propuestos a validar en la registración de incidencias.

* ID de incidente
* Estado
* Título/ breve descripción
* Categoría
* Servicio afectado
* Elemento de configuración
* Urgencia
* Impacto
* Prioridad
* Solicitante / Detección
* Grupo resolutor
* Tiempo estimado de trabajo
* Solución aplicada
* Fecha de inicio
* Fecha de cierre

# Prioridad, urgencia e impacto

**Urgencia**: Depende del tiempo máximo de demora aceptable para la resolución del incidente para el servicio afectado

|  |  |
| --- | --- |
| Urgencia | Criterio |
| *Alta* | Son Incidentes que deben ser resueltos inmediatamente ya que afecta seriamente la disponibilidad de un servicio crítico. La respuesta debe ser inmediata |
| *Media* | Son incidentes que requieren de solución lo antes posible, se corre el riesgo de impactar el negocio. Son incidentes programables, no postergables. |
| *Baja* | Corresponde a Incidentes que pueden esperar por su solución. Es un Incidente que puede esperar al siguiente release. Es programable y postergable |

**Impacto**: Determina cómo afecta a los servicios de negocio y/o número de usuarios afectados. Está expresado en función de la complejidad técnica requerida para la solución del Incidente.

|  |  |
| --- | --- |
| Impacto | Criterio |
| *Mayor* | Tiene un impacto mayor en los clientes del servicio (les imposibilita su utilización) y requiere de una gran cantidad de recursos para su resolución. |
| *Moderado* | Cuenta con un requerimiento significativo de recursos para su resolución. |
| *Menor* | Su resolución es sencilla y no requiere de gran cantidad de recursos. |

**Prioridad**: es lasecuencia en la que un Incidente debe ser resuelto en relación al resto de los Incidentes pendientes, teniendo en cuenta la urgencia con que deben ser atendidos y el impacto.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PRIORIDAD | | IMPACTO | | |
| **Mayor** | **Moderado** | **Menor** |
| **URGENCIA** | **Alta** | **Critica** | **Alta** | **Media** |
| **Media** | **Alta** | **Media** | **Baja** |
| **Baja** | **Media** | **Baja** | **Baja** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Prioridad** | **Tiempo de Respuesta** | **Tiempo de Resolución** | **Objetivo cantidad de incidentes** |
| **Crítica** | Inmediata | < 4 horas | 3 Incidencias x mes |
| **Alta** | 1 Hora | < 8 horas | 15 Incidencias x mes |
| **Media** | 8 horas | < 24 horas | 20 Incidencias x mes |
| **Baja** | 24 horas | < 15 días | 30 Incidencias x mes |

## Definición de niveles de severidad

*Podemos intentar ir directamente a esto y solo explicar los motivos ?*

|  |  |
| --- | --- |
| **Nivel de Severidad** | **Características** |
| **Critico** | * Los servicios establecidos como críticos en el catálogo están caídos, seriamente impactados o no están disponibles. * Incumplimiento de SLA |
| **Alta** | * Los servicios están caídos, seriamente impactados o no están disponibles. * El impacto del negocio es alto o severo. * El compromiso de los recursos necesarios es alto para la resolución |
| **Media** | * Los servicios están degradados o poco fiables. * El impacto del negocio es medio en términos del cliente |
| **Baja** | * El rendimiento de los servicios y acuerdos no están en riesgo. * El impacto en el negocio actual es baja * No existe el compromiso de los recursos de gestión de incidentes |

# Estados de los incidentes

Los incidentes podrán pasar por diferentes estados, que permitirán reconocer el grado de avance de las actividades de solución de los mismos.

* **Abierto**: El incidente se encuentra abierto, asignado a un grupo resolutor
* **En progreso**: El incidente tiene un analista o especialista asignado el cual está notificado y comienza a correr el tiempo para su resolución
* **Pendiente de xxx**: No está en manos del analista y se espera la intervención de otra persona para continuar con la resolución.
* **Pendiente del proveedor**: Incidente a la espera de respuesta por parte del proveedor externo del servicio
* **Cancelado:** Se desestima el incidente cargado
* **Cerrado**: El incidente ha sido resuelto
* **Cerrado-Aprobado**: El incidente resuelto se ha validado por el coordinador.

# RIO (reunión de incidentes operativos)

Se recomienda realizar esta reunión en forma quincenal ver de complementar OTRA que ya se realice y tendrá como objetivo la revisión de los incidentes de severidad críticos y alta, ocurridos en ese periodo de tiempo, y los 5 incidentes que más se repiten en los últimos 60 dias. La principal función de la RIO es impulsar la comunicación fluida entre los diferentes actores de los servicios y la gestión de incidentes

# Control y mejora continua

## Métricas:

#### KPI recomendados

* Incidentes pendientes de resolución
* Porcentaje de incidentes resueltos por grupo de resolución
* Cantidad y porcentaje de incidentes resueltos por Nivel 1
* Cantidad y porcentaje de incidentes resueltos sin ser derivados a otros grupos de resolución
* Cantidad de incidentes registrados por servicios
* Porcentaje de incidentes críticos

#### Reportes recomendados

* Top 10 de incidentes por categoría
* Cantidad de incidentes cerrados y no confirmados
* Informe de cierre de incidentes críticos
* Reporte de incidentes para la RIO. Incidentes críticos, incidentes de prioridad Alta y top 5 de repetitivos

How incident management works

Incident management is about understanding the incident life cycle and the actions to take at each stage.

Incident process

**Inputs to the incident process**

.Incident details logged at the service desk

.Configuration details from the configuration management database

.Output from problem management and known errors

.Resolution details from other incidents

.Responses to requests for change

**Output from the incident process**

.Incident resolution and closure

.Updated incident record and call log

.Methods for work arounds

.Communication with the user

.Requests for change

.Management information (reports)

.Input to the problem management process

**Activities of the incident process**

.Incident detection and recording

.Initial user support by the single point of contact (service desk)

.Investigation and diagnosis

Resolution and recovery of service

.Incident closure

.Incident ownership, monitoring, and communication

**Define what needs to be done to implement incident management**

.Before identifying your needs, consider what you want to achieve

.This is an opportunity to re-evaluate the way you have, to date, approached and fixed incidents. Rethink current processes and activities

.Understand the difference between incident management and problem management

.Technical staff will always try to solve the cause of a problem. Their way of thinking needs to change so that they approach it with incident management before problem management

.Choose which areas to improve and which processes to remove

.You need to sell the idea to the other staff, so make it appeal to yourself first

**4.2.1 Purpose/goal/objective**

The primary goal of the Incident Management process is

to restore normal service operation as quickly as possible

and minimize the adverse impact on business operations,

thus ensuring that the best possible levels of service

quality and availability are maintained. ‘Normal service

operation’ is defined here as service operation within

* SLA limits.

**4.2.2 Scope**

Incident Management includes any event which disrupts,

or which could disrupt, a service. This includes events

which are communicated directly by users, either through

the Service Desk or through an interface from Event

Management to Incident Management tools.

Incidents can also be reported and/or logged by technical

staff (if, for example, they notice something untoward with

a hardware or network component they may report or log

an incident and refer it to the Service Desk). This does not

mean, however, that all events are incidents. Many classes

of events are not related to disruptions at all, but are

indicators of normal operation or are simply informational

(see section 4.1).

Although both incidents and service requests are reported

to the Service Desk, this does not mean that they are the

same. Service requests do not represent a disruption to

agreed service, but are a way of meeting the customer’s

needs and may be addressing an agreed target in an SLA.

Service requests are dealt with by the Request Fulfilment

process (see section 4.3).

**4.2.3 Value to business**

The value of Incident Management includes:

■ The ability to detect and resolve incidents, which

results in lower downtime to the business, which in

turn means higher availability of the service. This

means that the business is able to exploit the

functionality of the service as designed.

■ The ability to align IT activity to real-time business

priorities. This is because Incident Management

includes the capability to identify business priorities

and dynamically allocate resources as necessary.

■ The ability to identify potential improvements to

services. This happens as a result of understanding

what constitutes an incident and also from being in

contact with the activities of business operational staff.

■ The Service Desk can, during its handling of incidents,

identify additional service or training requirements

found in IT or the business.

Incident Management is highly visible to the business, and

it is therefore easier to demonstrate its value than most

areas in Service Operation. For this reason, Incident

Management is often one of the first processes to be

implemented in Service Management projects. The added

benefit of doing this is that Incident Management can be

used to highlight other areas that need attention –

thereby providing a justification for expenditure on

implementing other processes.

**4.2.4 Policies/principles/basic concepts**

There are some basic things that need to be taken into

account and decided when considering Incident

Management. These are covered in this section.

***4.2.4.1 Timescales***

Timescales must be agreed for all incident-handling stages

(these will differ depending upon the priority level of the

incident) – based upon the overall incident response and

resolution targets within SLAs – and captured as targets

within OLAs and Underpinning Contracts (UCs). All support

groups should be made fully aware of these timescales.

Service Management tools should be used to automate

timescales and escalate the incident as required based on

pre-defined rules.

The Incident Model should include:

■ The steps that should be taken to handle the incident

■ The chronological order these steps should be taken

in, with any dependences or co-processing defined

■ Responsibilities; who should do what

■ Timescales and thresholds for completion of the

actions

■ Escalation procedures; who should be contacted and

when

■ Any necessary evidence-preservation activities

(particularly relevant for security- and capacity-related

incidents).

***4.2.4.3 Major incidents***

A separate procedure, with shorter timescales and greater

urgency, must be used for ‘major’ incidents. A definition of

what constitutes a major incident must be agreed and

ideally mapped on to the overall incident prioritization

system – such that they will be dealt with through the

major incident process.

***4.2.5.2 Incident logging***

The information needed for each incident is likely to

include:

■ Unique reference number

■ Incident categorization (often broken down into

between two and four levels of sub-categories)

■ Incident urgency

■ Incident impact

■ Incident prioritization

■ Date/time recorded

■ Name/ID of the person and/or group recording the

incident

■ Method of notification (telephone, automatic, e-mail,

in person, etc.)

■ Name/department/phone/location of user

■ Call-back method (telephone, mail, etc.)

■ Description of symptoms

■ Incident status (active, waiting, closed, etc.)

■ Related CI

■ Support group/person to which the incident is

allocated

■ Related problem/Known Error

■ Activities undertaken to resolve the incident

■ Resolution date and time

■ Closure category

■ Closure date and time.

Note: If the Service Desk does

***4.2.5.3 Incident categorization***

Part of the initial logging must be to allocate suitable

incident categorization coding so that the exact type of

the call is recorded. This will be important later when

looking at incident types/frequencies to establish trends

for use in Problem Management, Supplier Management

and other ITSM activities.

***4.2.5.4 Incident prioritization***

Another important aspect of logging every incident is to

agree and allocate an appropriate prioritization code – as

this will determine how the incident is handled both by

support tools and support staff

***4.2.5.5 Initial diagnosis***

If the incident has been routed via the Service Desk, the

Service Desk Analyst must carry out initial diagnosis,

typically while the user is still on the telephone – if the

call is raised in this way – to try to discover the full

symptoms of the incident and to determine exactly what

has gone wrong and how to correct it. It is at this stage

that diagnostic scripts and known error information can be

most valuable in allowing earlier and accurate diagnosis.

If possible, the Service Desk Analyst will resolve the

incident while the user is still on the telephone – and

close the incident if the resolution is successful.

If the Service Desk Analyst cannot resolve the incident

while the user is still on the telephone, but there is a

prospect that the Service Desk may be able to do so

within the agreed time limit without assistance from other

support groups, the Analyst should inform the user of their

intentions, give the user the incident reference number

and attempt to find a resolution.

***4.2.5.6 Incident escalation***

■ **Functional escalation**. As soon as it becomes clear

that the Service Desk is unable to resolve the incident

itself (or when target times for first-point resolution

have been exceeded – whichever comes first!) the

incident must be immediately escalated for further

support.

**Hierarchic escalation**. If incidents are of a serious

nature (for example Priority 1 incidents) the

appropriate IT managers must be notified, for

informational purposes at least. Hierarchic escalation is

also used if the ‘Investigation and Diagnosis’ and

‘Resolution and Recovery’ steps are taking too long or

proving too difficult. Hierarchic escalation should

continue up the management chain so that senior

managers are aware and can be prepared and take

any necessary action, such as allocating additional

resources or involving suppliers/maintainers. Hierarchic

escalation is also used when there is contention about

to whom the incident is allocated.

***4.2.5.8 Resolution and Recovery***

When a potential resolution has been identified, this

should be applied and tested. The specific actions to be

undertaken and the people who will be involved in taking

the recovery actions may vary, depending upon the nature

of the fault – but could involve:

***4.2.5.9 Incident Closure***

The Service Desk should check that the incident is fully

resolved and that the users are satisfied and willing to

agree the incident can be closed. The Service Desk should

also check the following:

■ **Closure categorization**. Check and confirm that the

initial incident categorization was correct or, where

the categorization subsequently turned out to be

incorrect, update the record so that a correct closure

categorization is recorded for the incident – seeking

advise or guidance from the resolving group(s) as

necessary.

■ **User satisfaction survey**. Carry out a user satisfaction

call-back or e-mail survey for the agreed percentage of

incidents.

■ **Incident documentation**. Chase any outstanding

details and ensure that the Incident Record is fully

documented so that a full historic record at a

sufficient level of detail is complete.

**4.2.6 Triggers, input and output/interprocess**

**Interfaces**

**Problem Management**

**Configuration Management**

**Change Management**

**Capacity Management**:

**Availability Management**

**Service Level Management**

**4.2.7 Information Management**

Most information used in Incident Management comes

from the following sources

**The Incident Management tools**, which contain

information about:

● Incident and problem history

● Incident categories

● Action taken to resolve incidents

● Diagnostic scripts which can help first-line analysts

to resolve the incident, or at least gather

information that will help second- or third-line

analysts resolve it faster.

■ **Incident Records**, which include the following data:

● Unique reference number

● Incident classification

● Date and time of recording and any subsequent

activities

● Name and identity of the person recording and

updating the Incident Record

● Name/organization/contact details of affected

user(s)

● Description of the incident symptoms

● Details of any actions taken to try to diagnose,

resolve or re-create the incident

● Incident category, impact, urgency and priority

● Relationship with other incidents, problems,

changes or Known Errors

● Closure details, including time, category, action

taken and identity of person closing the record.

Incident Management also requires access to the CMS.

This will help it to identify the CIs affected by the incident

and also to estimate the impact of the incident.

The Known Error Database provides valuable information

about possible resolutions and workarounds. This is

discussed in detail in paragraph 4.4.7.2.

**4.2.8 Metrics**

The metrics that should be monitored and reported upon

to judge the efficiency and effectiveness of the Incident

Management process, and its operation, will include:

■ Total numbers of Incidents (as a control measure)

■ Breakdown of incidents at each stage (e.g. logged,

work in progress, closed etc)

■ Size of current incident backlog

■ Number and percentage of major incidents

■ Mean elapsed time to achieve incident resolution or

circumvention, broken down by impact code

**4.2.9 Challenges, Critical Success Factors**

**and risks**

***4.2.9.1 Challenges***

The following challenges will exist for successful Incident

Management:

■ The ability to detect incidents as early as possible. This

will require education of the users reporting incidents,

the use of Super Users (see paragraph 6.2.4.5) and the

configuration of Event Management tools.

■ Convincing all staff (technical teams as well as users)

that all incidents must be logged, and encouraging

the use of self-help web-based capabilities (which can

speed up assistance and reduce resource

requirements).

■ Availability of information about problems and Known

Errors. This will enable Incident Management staff to

learn from previous incidents and also to track the

status of resolutions.

■ Integration into the CMS to determine relationships

between CIs and to refer to the history of CIs when

performing first-line support.

■ Integration into the SLM process. This will assist

Incident Management correctly to assess the impact

and priority of incidents and assists in defining and

executing escalation procedures. SLM will also benefit

from the information learned during Incident

Management, for example in determining whether

service level performance targets are realistic and

achievable.

***4.2.9.2 Critical Success Factors***

The following factors will be critical for successful Incident

Management:

■ A good Service Desk is key to successful Incident

Management

■ Clearly defined targets to work to – as defined in SLAs

■ Adequate customer-oriented and technically training

support staff with the correct skill levels, at all stages

of the process

■ Integrated support tools to drive and control the

process

■ OLAs and UCs that are capable of influencing and

shaping the correct behaviour of all support staff.

***4.2.9.3 Risks***

The risks to successful Incident Management are actually

similar to some of the challenges and the reverse of some

of the Critical Success Factors mentioned above. They

include:

■ Being inundated with incidents that cannot be

handled within acceptable timescales due to a lack of

available or properly trained resources

■ Incidents being bogged down and not progressed as

intended because of inadequate support tools to raise

alerts and prompt progress

■ Lack of adequate and/or timely information sources

because of inadequate tools or lack of integration

■ Mismatches in objectives or actions because of poorly

aligned or non-existent OLAs and/or UCs.