MARCO de CIBERSEGURIDAD

GLOSARIO

Uruguay Presidencia

agesic

SEGURIDAD DE LA INFORMACIÓN

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

1. Objetivo y alcance

En este documento se presentan las abreviaciones y definiciones utilizadas en el Marco de ciberseguridad, así como en la Guía de implementación.

2. Glosario

2.1 Abreviaturas

ABM	Altas Bajas Modificaciones
BIA	Business Impact Analysis
CAdES CMS	Advanced Electronic Signatures is a set of extensions to Cryptographic Message Syntax (CMS) signed data making it suitable for advanced electronic signatures.
CCTV	Closed Circuit Television (Circuito Cerrado de Televisión)
CDA	Clinical Document Architecture (Arquitectura de Documento Clínico)
CERTuy	Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay
CPD	Centro de Procesamiento de Datos. Centro de datos. Data center.
CSI	Comité de Seguridad de la Información
CSIRT	Computer Security Incident Response Team (Equipo de Respuesta ante Incidentes de Seguridad Informática)
DLP	Data Loss Prevention
DNS	Domain Name System (Sistema de Nombres de Dominio)
EMG	Estándar Mínimo de Gestión (Banco Central de Uruguay)
HCE	Historia Clínica Electrónica
HCEN	Historia Clínica Electrónica Nacional
HIS	Hospital Information System (Sistema de Información Hospitalaria)
HTTPS	Hypertext Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)
HSM	Hardware Security Module (Módulo de Seguridad Hardware)

ICMP	Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)
IP	Internet Protocol (Protocolo IP)
IPS	Intrusion Prevention System (Sistema de Prevención de Intrusos)
LAN	Local Area Network (Red de Área Local)
LIS	Laboratory Information System (Sistema de Información de Laboratorio)
MUA	Mail User Agent (Agente de Usuario de Correo)
MTA	Mail Transfer Agent (Agente de Transferencia de Correo)
PACS	Picture Archiving and Communication System (Sistema de Archivo y Transmisión de Imágenes)
PGP	Pretty Good Privacy (Privacidad Bastante Buena)
RSI	Responsable de la Seguridad de la Información
SAN	Storage Area Network (Red de Área de Almacenamiento)
SI	Seguridad de la Información
SGSI	Sistema de Gestión de Seguridad de la Información
SLA	Service Level Agreement (Acuerdo de Nivel de Servicio)
SNMP	Simple Network Management Protocol (Protocolo Simple de Administración de Red)
SO	Sistema Operativo
SSL	Secure Sockets Layer (Capa de Puertos Seguros)
TCP/IP	Transmission Control Protocol and the Internet Protocol (Protocolo de control de transmisión/Protocolo de Internet)
TI	Tecnología de la Información
TIC	Tecnología de la Información y la Comunicación
TLS	Transport Layer Security (Seguridad de la Capa de Transporte)
UCE	Unidad de Certificación Electrónica
UE	Unidad Ejecutora
RTO	Recovery Time Objective (Tiempo de Recuperación Objetivo)
RPO	Recovery Point Objective (Punto de Recuperación Objetivo)
URCDP	Unidad Reguladora y de Control de Datos Personales

VPN	Virtual Private Network (Red Privada Virtual)
WAF	Web Application Firewall
WIFI	Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica
WRT	Work Recovery Time (Tiempo de Recuperación de Trabajo)
XADES	XML Advanced Electronic Signatures (Firma electrónica avanzada XML)
XDS	Cross-Enterprise Document Sharing (Intercambio de Documentos entre Empresas)
XML	Extensible Markup Language (Lenguaje de Marcado Extensible)

2.2 Definiciones

A

Acceso privilegiado
Cuando se requiere acceso a funciones de administración de usuarios, roles, grupos y perfiles (creación, modificación, bloqueo e inactivación de cuentas de usuario) y/o parametrización (cambios a los parámetros de configuración, tablas básicas, archivos de configuración).

Activos de información
Son aquellos datos o información que tienen valor para el organismo. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones].

Por ejemplo: software, hardware, servicios de nube, etc.

Activos de información críticos del Estado
Son aquellos activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios vitales para la operación del gobierno y la economía del país. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]

Amenaza
Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema o en una organización. [ISO/IEC 27000:2009]

Antivirus
Sistemas informáticos cuyo objetivo es detectar o eliminar virus informáticos.

Antispyware
Sistema informático que permite detectar o eliminar spyware (programas espías) que transmiten información a una entidad externa sin el conocimiento o consentimiento del usuario.

Áreas seguras o protegidas

Áreas donde se procesa y almacena la información y/o respaldos; por ejemplo, centro de datos y archivos.

B

BIA (del inglés Business Impact Analysis)
Un análisis de impacto en el negocio está orientado a identificar qué procesos de negocio podrían verse afectados y de qué forma, ante la materialización de los riesgos identificados. Sus objetivos principales son identificar los procesos críticos del negocio y definir su prioridad en función del impacto relacionado a una interrupción (organizacional, financiero, de imagen, etc.) para la organización.

C

Cadena de suministro
Sistema organizacional, personas, actividades, información y recursos, posiblemente de alcance internacional, que proporciona productos o servicios a los consumidores. [NIST SP 800-53 Rev. 4 - “Supply Chain” Page B-19]

CAdES
CMS Advanced Electronic Signatures
Conjunto de extensiones a los datos firmados con CMS Cryptographic Message Syntax (Sintáxis de Mensajes Criptográficos) que lo hacen adecuado para firmas electrónicas avanzadas.

CCTV
Closed Circuit Television (Circuito Cerrado de Televisión).
Tecnología de videovigilancia diseñada para supervisar una diversidad de ambientes y actividades.

CDA
Clinical Document Architecture (Arquitectura de Documento Clínico).
Documento intercambiable en los procesos de interoperabilidad. Corresponde a los actos clínicos o eventos en salud que se registran en la institución prestadora de los servicios de salud, y que pueden ser compartidos o intercambiados acorde con la dinámica establecida y a las políticas de seguridad de la información del marco jurídico.

CERTuy
El CERTuy es el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay. Un CERT (del inglés Computer Emergency Response Team / Coordination Center) es un equipo de respuesta y un centro de coordinación de emergencias informáticas. [Sitio oficial del CERTuy: www.cert.uy]

Código móvil
Programas de software o partes de programas obtenidos de sistemas de información remoto, transmitidos a través de una red y ejecutados en un sistema de información local sin instalación o ejecución explícita por parte del destinatario (por ejemplo, un agente o una macro de un documento). [NIST SP 800-53 Rev. 4 - “Mobile code” p93]

Control
Medio de gestionar el riesgo, incluyendo políticas, procedimientos, guías, prácticas o estructuras organizativas, que pueden ser de naturaleza administrativa, técnica, de gestión, o legal. [UNIT-ISO/IEC 27000:2013]

D

DNS Domain Name System (Sistema de Nombres de Dominio)
Sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

E

Ethical hacking (hackeo ético)
Utilización de técnicas de ataque para encontrar fallas de seguridad, realizas con el permiso de la organización, con el fin de mejorar la seguridad.

Evento de seguridad informática
Es una ocurrencia identificada de un estado de un sistema, servicio o red que indica que una posible violación de la política de seguridad de la información, la falla de medidas de seguridad o una situación previamente desconocida, que pueda ser relevante para la seguridad. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]

F

Factor de doble autenticación
Medida de seguridad que frecuentemente requiere de un código obtenido a partir por ejemplo de una aplicación, un dispositivo o un mensaje SMS, además de una contraseña para acceder al servicio.

H

HASH
Algoritmo que, a partir de una entrada (texto, archivo, etc.) crea una salida alfanumérica que representa un resumen de toda la información de entrada y que solo puede crearse nuevamente con la misma información.

HCE
Historia Clínica Electrónica
Es el conjunto integral de datos clínicos, sociales y económicos, referidos a la salud de una persona, desde su nacimiento hasta su muerte, procesados a través de medios electrónicos, siendo el equivalente funcional de la historia clínica papel.

HCEN
Historia Clínica Electrónica Nacional
Plataforma de Historia Clínica Electrónica Nacional. Es la infraestructura tecnológica y de servicios que permite la conectividad de los diferentes sistemas de información del conjunto de Instituciones con competencias legales en materia de salud, públicas y privadas, con el objetivo de intercambiar información clínica.

HIS
Hospital Information System (Sistema de Información Hospitalaria)
Sistema de Información Hospitalaria, también conocido como sistema de

información en salud. Este sistema apoya a las instituciones de salud en la gestión de las actividades operativas, tácticas y estratégicas.

HSM
Hardware Security Module (Módulo de Seguridad Hardware)
Dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.

HTTPS
Hypertext Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)
Protocolo de aplicación basado en el protocolo HTTP (Hyper Text Transfer Protocol), destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

I

ICMP Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)
Es un subprotocolo de control y notificación de errores del Protocolo de Internet (IP). Es utilizado para enviar mensajes de error, indicando por ejemplo que un enrutador o host no puede ser localizado.

Incidente de seguridad de la información
Un incidente de seguridad de la información es indicado por un único o una serie de eventos indeseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información. [ISO/IEC 27035:2011]

Incidente de seguridad informática
Es una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que compromete la seguridad de un sistema (confidencialidad, integridad o disponibilidad). [Decreto N° 451/009 de 28 de Setiembre 2009- Art.3 Definiciones]

Información sensible
Información personal privada de un individuo tales como contraseñas, información personal que revele origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

IP Internet Protocol (Protocolo de Internet)
Número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión)
de un dispositivo (computadora, tableta, portátil, teléfono inteligente) que utilice el protocolo IP, que corresponde al nivel de red del modelo TCP/IP.

IPS Intrusion Prevention System (Sistema de Prevención de Intrusos)
Software que ejerce el control de acceso en una red informática para proteger a los sistemas ante ataques y abusos.

L

Línea base
Una especificación o producto que se ha revisado formalmente y sobre los que se ha llegado a un acuerdo, y que de ahí en adelante sirve como base para un desarrollo posterior y que puede cambiarse solamente a través de procedimientos formales de control de cambios. [IEEE 610.12/1990]

LIS Laboratory Information System (Sistema de Información de Laboratorio)
También conocido como LIMS Laboratory Information Management System (Sistema de Gestión de Información de Laboratorio). Es un sistema que soporta por ejemplo la gestión del flujo de trabajo en laboratorios de análisis clínicos desde el seguimiento de muestras hasta múltiples aspectos de la informática de laboratorios.

LOG Historial de log o registro
Registro de todos los acontecimientos, eventos o acciones que afectan un proceso informático en particular y constituye una evidencia del comportamiento del sistema.

M

mod_security
Es un módulo del servidor Web Apache que provee protección contra diversos ataques hacia aplicaciones Web y permite monitorizar tráfico HTTP, así como realizar análisis en tiempo real sin necesidad de hacer cambios a la infraestructura existente.

MTD Maximum Tolerable Downtime (Tiempo de inactividad máximo tolerable).
Se trata de la cantidad máxima de tiempo que una organización puede estar sin operar sin causar daños irreparables al negocio.
MTD = RTO + WRT

P

PACS Picture Archiving and Communication System (Sistema de Archivo y Transmisión de Imágenes)
Sistema computarizado para el archivo digital de imágenes médicas.

Personal
En el ámbito de la administración central, hace referencia a personal presupuestado, contratado, pasantes, no incluye proveedores de servicio.

PGP Pretty Good Privacy (Privacidad Bastante Buena)
Programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

Plan de respuesta a incidentes
Este documento contiene, además del procedimiento de respuesta a incidentes, la planificación de la respuesta, por ejemplo: introducción, roles y responsabilidades, metodología, fases de las respuestas a incidentes, plan de comunicación, documentación, etc.

Propietario de activos
El término propietario identifica un individuo o entidad que ha probado habilidades de gestión para controlar la producción, desarrollo, mantenimiento, uso y seguridad de un activo. El término propietario no significa que la persona tiene efectivamente derechos de propiedad sobre el activo. [Agesic (políticas marco, políticas del SGSI, políticas de Presidencia – Manual de Políticas de Seguridad de la Información / Gestión de Activos / Responsabilidad sobre los activos]

R

Red Salud
Es una red privada para la conexión de Instituciones con competencias legales en la materia de salud, públicas y privadas, a través de la Plataforma de Historia Clínica Electrónica Nacional, que permite el intercambio seguro de información de los usuarios del sistema de salud.

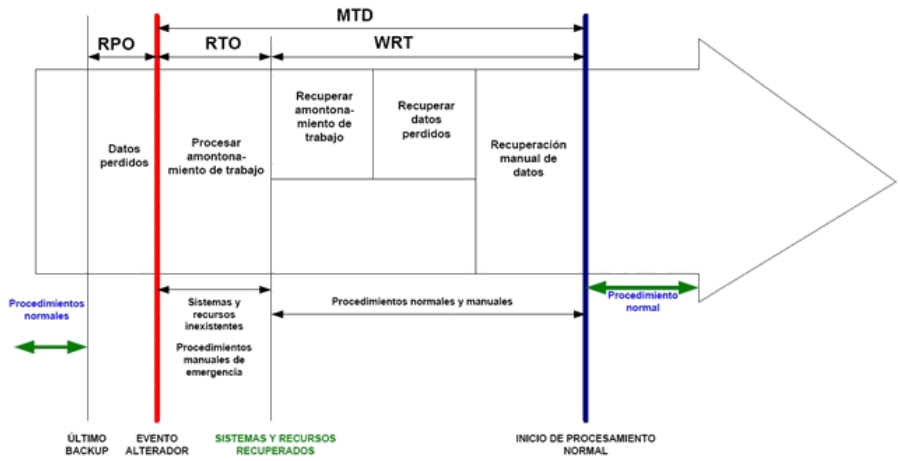
Remediación de incidente
Consiste en las actividades necesarias de reparación o mitigación realizadas para subsanar la causa raíz que viabilizó un incidente o vulnerabilidad detectadas en sistemas o procesos.

RIS Radiology Information System (Sistema de Información de Radiología)
Sistema para la gestión y el control del diagnóstico por imagen (por ejemplo, turnos, insumos, facturación, informes de diagnóstico, estadísticas). Habitualmente conectado a los sistemas HIS y PACS.

Router (Enrutador)
Dispositivo que proporciona conectividad a nivel de capa 3 o capa de red del modelo OSI Open System Interconection (Sistema Abierto de Interconexión).

RPO Recovery Point Objective (Punto de Recuperación Objetivo)
La máxima cantidad de información que se puede perder de acuerdo al cronograma de realización de copias de respaldo y/o necesidades de información que se presenten. En otras palabras, indica el tiempo máximo que una organización acepta respecto a pérdida de datos desde el último respaldo. Por ejemplo, las transacciones de hasta cuánto tiempo atrás se está dispuesto a perder o reintroducir al sistema.

RTO Recovery Time Objective (Tiempo de Recuperación Objetivo)
Tiempo requerido para que los sistemas críticos de la Organización estén nuevamente operando. En otras palabras, indica la cantidad de tiempo en que se puede realmente recuperar los procesos en caso de disrupción.
Se busca siempre que los tiempos de los RTOs sean menores que los de los MTDs.



S

Sistema informático
Los ordenadores y redes de comunicación electrónica, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento. [Decreto N° 451/009 de 28 de Setiembre 2009- Art.3 Definiciones]

SLA (del inglés Service Level Agreement)
Acuerdo negociado entre dos partes, una cliente y otra proveedora, donde se definen puntos comunes de entendimiento sobre servicios, prioridades, responsabilidades y garantías. Incluye elementos tales como definición de los servicios, garantías y finalización del acuerdo, medición del rendimiento, gestión de problemas, obligaciones de las partes, entre otros.

Smart Card (Tarjeta inteligente)
Tarjeta inteligente con circuitos integrados, que permite la ejecución de cierta lógica programada.

SNMP Simple Network Management Protocol (Protocolo Simple de Administración de Red)
Protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

Software de aplicación
Programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos.

Software de base
Software que sirve para controlar e interactuar con el sistema operativo, proporcionando control sobre el hardware y dando soporte a otros programas, incluyendo el propio sistema operativo.

Switch (Conmutador)
Dispositivo digital lógico de interconexión de equipos que opera a nivel de capa 2 o capa de enlace de datos (del modelo OSI).

T

TCP/IP
Transmission Control Protocol (TCP) and the Internet Protocol (IP)
Protocolo de control de transmisión/Protocolo de Internet
Descripción de protocolos de red desarrollado por Vinton Cerf y Robert E. Kahn, en la década de 1970.

TLS Transport Layer Security (Seguridad de la Capa de Transporte)
Protocolo criptográfico que proporciona comunicaciones seguras por una red.

Token
Dispositivo electrónico que se le da a un usuario autorizado de un servicio informático para facilitar el proceso de autenticación.

U

UCE
Unidad de Certificación Electrónica
Creada por el artículo 12 de la Ley N° 18.600 de Documento Electrónico y Firma Electrónica, como un órgano desconcentrado de Agesic. Sus cometidos y funciones son: acreditación, control, instrucción, regulación y sanción.

URCDP
Unidad Reguladora y de Control de Datos Personales
Unidad creada por la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data (LPDP), con autonomía técnica, cuya competencia es custodiar el cumplimiento de la legislación de protección de datos personales y asegurar el respeto de sus principios.

Usuario privilegiado
Usuario que requiere acceso privilegiado para realizar funciones específicas. Es aquel que tiene autorización administrativa. Usuario con rol administrador.

V

VPN Virtual Private Network (Red Privada Virtual)
Tecnología de red de computadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

Vulnerabilidad
Debilidad de un activo o control que puede ser explotada por una amenaza. [ISO/IEC 27000:2009]

W

WAF (del inglés Web Application Firewall)
Un Firewall de Aplicaciones Web es un dispositivo de hardware o software que permite proteger los servidores de aplicaciones Web de determinados ataques específicos en Internet.

Webmail
Un Webmail o correo Web es un cliente de correo electrónico, que provee una interfaz Web por la que accede al correo electrónico.

WRT Work Recovery Time (Tiempo de Recuperación de Trabajo)
Tiempo requerido para recuperar la información perdida (Basado en el RPO), así como de ingresar al sistema todos los datos que se generaron durante la caída del sistema.

X

XADES XML Advanced Electronic Signatures (Firma electrónica avanzada XML)
Es un conjunto de extensiones a las recomendaciones XML-DSig (Firma XML; recomendación del W3C World Wide Web Consortium que define una sintaxis XML para la firma digital haciéndolas adecuadas para la firma electrónica avanzada).

XDS Cross-Enterprise Document Sharing (Intercambio de Documentos entre Empresas)
Especificación basada en estándares para administrar el intercambio de documentos entre cualquier empresa de atención médica, desde un consultorio médico privado hasta una clínica, un centro de cuidados intensivos para pacientes internados y sistemas de registros de salud personales.

XML Extensible Markup Language (Lenguaje de Marcado Extensible)
Meta-lenguaje que permite definir lenguajes de marcas desarrollado por el World Wide Web Consortium (W3C) utilizado para almacenar datos en forma legible.

X.509 v3
Estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI). X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación. La última versión es la 3, de mayo de 2008.