



**Análisis de Riesgo
de Tecnología Informática y los
Sistemas Computadorizados de
Información de la Escuela de Artes
Plásticas y Diseño**

Revisado septiembre 2021

Tabla de Contenido

I.	Introducción	2
II.	Base Legal	2
III.	Objetivos del plan.....	3
IV.	Alcance.....	3
V.	Estructura administrativa de la OSI.....	3
	Organigrama de la OSI.....	3
	Tabla I: Personal de la OSI.....	4
VI.	Facilidades físicas de la OSI.....	4
VII.	Análisis de riesgo	5
VIII.	Actividades de recuperación	6
IX.	Suplidores	7
	Tabla II: Aplicaciones.....	7
X	Desalojo de la Oficina de Sistemas de Información	8
XI	Descripción del equipo localizado en la OSI.....	8
	Tabla III: Descripción Equipo OSI.....	8
XII	Aplicaciones en la nube administradas por la OSI.....	8
	Tabla IV: Servicios y aplicaciones en la nube	9
XIII.	Red de comunicaciones	10
XIV.	Contraseñas	10
XV.	Clasificación del equipo y los datos	10
	Tabla V: Inventario de switches en la red.....	10
XVI	Procedimientos de resguardo y recuperación.....	11
XVII.	Medidas preventivas	11
XVIII.	Actualización.....	12
Anejo I	13
Reporte de Incidente de Seguridad de la Información	13

I. Introducción

La Corporación de la Escuela de Artes Plásticas y Diseño ha aumentado significativamente el uso de la tecnología. Todas las oficinas administrativas dependen de un sistema robusto y estructurado para la continuidad de sus operaciones. Este informe de Análisis de Riesgo en conjunto con el Plan de Continuidad es una guía clara de los sistemas que operan actualmente en la Institución. Muestra cuáles son los riesgos asociados a la ubicación y situaciones ambientales e imprevistas que pudieran afectar el buen desempeño.

La dependencia en la tecnología informática aumenta grandemente la efectividad y la eficiencia de las operaciones la EAPD, mientras que la ausencia de estas herramientas afectaría negativamente dichas operaciones.

II. Base Legal

1. Ley Núm. 54 de 22 de agosto de 1990, según enmendada para crear la Escuela de Artes Plásticas y Diseño de Puerto Rico como entidad autónoma, adscrita al Instituto de Cultura Puertorriqueña. Posteriormente la Ley 225 que cambia la Escuela de Artes Plásticas y Diseño a Corporación pública e incorpora la palabra diseño en su nombre.
2. Ley número 151 de 22 de junio de 2004, según enmendada, "Ley de Gobierno Electrónico".
3. Ley número 229 de 2 de septiembre de 2003. "Ley para Garantizar el Acceso de Información a las Personas con Impedimentos".
4. Carta circular número 77-05 emitida por la Oficina de Gerencia y Presupuesto el 8 de diciembre de 2004, la cual establece políticas sobre diversos asuntos de tecnologías de información, y además deroga la Carta circular 96-01 del 25 de septiembre de 1995, así como las circulares emitidas a su amparo.
5. Carta circular número OC-98-11, emitida por la Oficina del Contralor de Puerto Rico el 18 de mayo de 1998, la cual sugiere algunas normas y controles para el uso del sistema computadorizado.
6. Carta circular número OC-06-13, emitida por la Oficina del Contralor de Puerto Rico el 28 de noviembre de 2005, la cual sugiere algunas normas y controles para el uso del sistema computadorizado, y además deroga la Carta circular OC- 2002-02 del 16 de agosto de 2001.
7. Puerto Rico Innovation and Technology Service (PRITS), mediante la Ley 75 del 25 de julio de 2019.

III. Objetivos del plan

1. Analizar los riesgos existentes que pudieran afectar la continuidad de las operaciones de la EAPD.
2. Analizar los controles implementados para proteger los activos.
3. Mantener informada a la gerencia sobre los riesgos existentes y sus posibles causas.

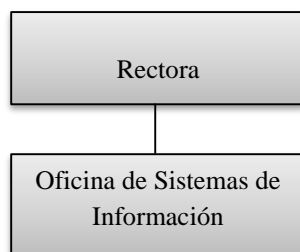
IV. Alcance

Este análisis aplica a todas las oficinas del EAPD donde existan computadoras, impresoras y otro equipo de tecnología informática, particularmente a la Oficina de Sistemas de Información (OSI).

V. Estructura administrativa de la OSI

La Oficina de Sistemas de Información de la EAPD responde directamente a la Entidad Nominadora. La misma consiste de una Oficial Principal de Informática y dos técnicos de computadoras. El organigrama es el siguiente:

Organigrama de la OSI



El horario de servicio del personal de la Oficina de Sistemas de Información es el siguiente:

Tabla I: Personal de la OSI

Nombre	Puesto	Horario	Teléfonos
Limaris Soto Aquino	Oficial Principal de Informática	8:30am – 5:00pm	787-725-8120 x381
Ariedwin Colón	Técnico de Computadoras	8:00am - 4:30pm	787-725-8120 x328
Carlos Cabrera	Técnico de Computadoras	7:30am – 4:00pm	787-725-8120 x352

VI. Facilidades físicas de la OSI

La Oficina de Sistemas de Información ocupa un área en el segundo piso del Edificio Antiguo Manicomio en la Escuela de Artes Plásticas y Diseño. Tiene los siguientes equipos:

1. Server Active Directory
2. Microtik de fibra óptica
3. 3 switches CISCO

En términos de seguridad la oficina tiene:

1. Una consola de aire acondicionado independiente de resguardo
2. Extintor de incendios de agua pulverizada. Estos son diseñados para proteger todas las áreas que contienen riesgos de fuegos Clase A (combustibles sólidos) y Clase C (equipos eléctricos energizados) en forma eficiente y segura. Tienen una boquilla de salida especialmente diseñada para producir una salida del agua en forma de niebla, que sumado a que el agente extintor es agua destilada, lo convierten en un agente extintor que no conduce la electricidad y además no daña los equipos electrónicos que no son atacados por el fuego.
3. La OSI tiene una batería de protección para el servidor Active Directory, cuyas especificaciones aparecen la Tabla III de este análisis. Cada cierto tiempo, el UPS lleva a cabo un auto cotejo ("self test") e informa el resultado a través de una pantalla y de bombillas. Además, se instaló un cable de "ground" para mayor seguridad en caso de cambios en el voltaje.
4. La Oficina ha identificado unas facilidades físicas alternas donde reiniciar las operaciones en caso de ocurrir un desastre que inutilice las actuales facilidades. Las mismas pertenecen al EAPD y están localizadas en el Edificio Antiguo

Hospital de la Concepción. Además, existe la alternativa de que los empleados se muevan a la modalidad de trabajo a distancia.

VII. Análisis de riesgo

A pesar de las medidas preventivas implantadas por la OSI, existe un alto riesgo de interrupción en las operaciones de dicha oficina. Este alto riesgo es provocado por las siguientes situaciones:

1. Edificio antiguo, con un alto riesgo de incendio ocasionado por el cableado eléctrico.
2. Edificio cercano al mar, lo que lo expone a vientos fuertes y un alto nivel de humedad y riesgo de inundación por un tsunami.
3. Riesgo de daños por los vientos y el agua de un huracán, particularmente debido a las condiciones débiles de las ventanas y las puertas.
4. Riesgo de daños al equipo y a las instalaciones eléctricas debido a filtraciones en el techo.
5. Riesgo de daños al equipo debido a las frecuentes interrupciones en el servicio eléctrico.
6. Riesgo de daños ocasionados por virus informáticos.

Las operaciones de informática confrontan una gran amenaza en lo referente a los riesgos anteriormente mencionados. Los riesgos asociados a eventos atmosféricos han sido disminuidos con la reciente impermeabilización del techo y la reparación de vigas, ventanas y puertas. La Administración está consciente de la importancia de ofrecer el mantenimiento adecuado a la infraestructura. El riesgo número cinco es atenuado por la existencia de sistemas de corriente ininterrumpida ("UPS"), tanto a nivel de la OSI como a nivel de los usuarios. También por la existencia de una Planta Eléctrica de 2 Kilos en el Edificio Antiguo Manicomio Insular y Generador 230 KW con voltaje 120/208 Trifásico en el Edificio Antiguo Hospital de la Concepción.

El riesgo número seis tiene una probabilidad menor de materializarse debido a las medidas preventivas ya implantadas al respecto, como las claves de acceso, el "firewall" Fortinet y los programas de detección de virus. Actualmente el sistema de seguridad de la EAPD es administrado por la compañía Worldnet a través de un contrato de mantenimiento.

En términos generales los riesgos han sido disminuidos ya que la agencia ha movido toda su operación a la nube. En la Tabla IV *Servicios y Aplicaciones en la nube*, se detallan los mismos. Los programas claves de Finanzas (MIP) y de Servicios Estudiantiles (Diamond) son manejados y monitoreados por las diferentes compañías que los producen. La agencia mantiene un contrato de servicios que asegura el resguardo de los datos y su rápida recuperación y acceso.

Los riesgos han sido explicados a la Gerencia, quienes han entendido la naturaleza de los mismos y su impacto en las operaciones. A tales efectos, han asignado presupuesto para implantar medidas que reduzcan la probabilidad de materializarse los mismos.

Los riesgos asociados a accesos a los datos y/o virus informáticos han sido atenuados por el uso de “firewalls”. De presentarse una situación donde pueda afectar la seguridad, la persona debe llenar el formulario de Reporte de Incidente de Seguridad. El Oficial Principal de Informática debe notificar a las agencias pertinentes de acuerdo con la Ley Núm. 97 del 2008 “Ley de Información al Ciudadano sobre Seguridad de Bancos de Información”, Anejo I.

VIII. Actividades de recuperación

Categoría 1: Pérdida de electricidad por causas de desastre natural. Las actividades para lograr la recuperación serán las siguientes:

- a. Reubicar el personal a un lugar con acceso al Internet. Los usuarios continuarían sus operaciones accediendo a los diferentes programas en la nube. Al tener dos edificios, uno de ellos sirve de lugar alternativo en caso de que el otro no esté disponible. De igual forma, se puede activar el trabajo a distancia según dispone la Oficina de Administración y Transformación de los Recursos Humanos del Gobierno de Puerto Rico (OATRH).
- b. Contactar a los proveedores de las aplicaciones, si fuera necesario.
- c. Probar el funcionamiento de las aplicaciones, así como la disponibilidad de los datos de cada una de ellas.
- d. Evaluar las causas de la pérdida de los datos y programas, y tomar las medidas necesarias para evitar la repetición de dicha pérdida

Categoría 2: Pérdida de datos, programas y servidores, pero sin daños a las facilidades físicas. Las actividades para lograr la recuperación serán las siguientes:

- a. Este riesgo es mínimo ya que todas las aplicaciones se encuentran en la nube y pueden ser accedidas desde cualquier lugar con acceso a Internet.

- b. Contactar a los suplidores de las aplicaciones, si fuera necesario.
- c. Probar el funcionamiento de las aplicaciones, así como la disponibilidad de los datos de cada una de ellas.

Categoría 3: Pérdida de datos, programas, así como graves daños a las facilidades físicas:

- a. Habilitar el lugar alternativo donde ubicará la OSI. Al tener dos edificios, uno de ellos sirve de lugar alternativo en caso de que el otro no esté disponible.

De igual forma, se puede activar el trabajo a distancia según dispone la Oficina de Administración y Transformación de los Recursos Humanos del Gobierno de Puerto Rico (OATRH).

- b. Probar el funcionamiento de las aplicaciones, así como la disponibilidad de los datos de cada una de ellas.
- c. Evaluar las causas de la pérdida de los datos y programas, así como los daños a las facilidades físicas, y tomar las medidas necesarias para evitar la repetición de las causas de dicha pérdida.

IX. Suplidores

Incluimos los nombres, las direcciones y los teléfonos de los suplidores principales del equipo y las aplicaciones utilizadas en el EAPD. De ser necesario, los mismos deberán ser contactados como parte de las actividades de recuperación.

Tabla II: Aplicaciones

APLICACIÓN	COMPAÑÍA	DESCRIPCIÓN	CONTACTO
DIAMONDD	DiamonDSis	Sistema de Información Estudiantil	Diamond SIS (HQ) 5023 North Parkway Calabasas Calabasas, CA 91302 +511 712 3990
MIP	Abila	Sistema de Finanzas	Call Sales: 800-811-0961 Main Office Phone: 800-647-3863 Main Office Location: 10800 Pecan Park Blvd., Suite 400, Austin, Texas 78750
KRONNOS	Interboro	Sistema de Asistencia	100 Grand Boulevard Paseos PMB 275 San Juan, PR 00926
ADP	ADP	Sistema de Nómina	Michael Schneider 973-974-5678 michael.schneider@adp.com Steve Cross 973-974-5744 steven.r.cross@adp.com

DESTINY	Follet Destiny	Sistema de catalogación de Biblioteca	Carretera núm. 1, Km 34.1, Reparto Industrial Cartagena, Caguas, Puerto Rico 00725 Mailing address: PO Box 6840, Caguas, PR 00726
GOOGLE APPS	Google Inc.	Correos electrónicos	https://support.google.com/accounts?hl=en#topic=3382296

X Desalojo de la Oficina de Sistemas de Información

La localización de la OSI permite un desalojo fácil y rápido de dicha oficina, pues provee varias alternativas para este propósito. Una de ellas consiste meramente en desalojar la oficina saliendo al patio interior. Este patio es lo suficientemente grande como para ofrecer protección temporera contra varios tipos de desastres. Una vez en el patio interior, las personas pueden desalojar el edificio del EAPD a través de cualquiera de los tres portones del Edificio.

XI Descripción del equipo localizado en la OSI

La Oficina de Sistemas de Información tiene en operación un servidor de gran capacidad con las siguientes descripciones:

Tabla III: Descripción Equipo OSI

Marca/Modelo	Número serial	Valor	Utilización
ProLiant DL380 Gen9 – rack mountable- 2U- 2way- 1x Xeon E5-2640V4/2.4 GHz Ram16GB RAM Hot Swap Hard Drive 1TB	Serial# MXQ752038Z	3,079.00	Active Directory

XII Aplicaciones en la nube administradas por la OSI

La EAPD no tiene aplicaciones físicas en su servidor. Todos sus servicios han sido contratados para poder acceder a través de la nube. De igual manera estos servicios están asegurados mediante contrato e incluye la realización de resguardo de datos. El riesgo asociado a la pérdida de datos se ha reducido sustancialmente descargando la responsabilidad a terceros con sistemas más robustos y dedicados a la protección de los sistemas.

Tabla IV: Servicios y aplicaciones en la nube

Aplicación	Compañía	Descripción y costo anual	Contacto
DiamondD	DiamonDSis	Sistema de Información Estudiantil \$14,000	Diamond SIS (HQ) 5023 North Parkway Calabasas Calabasas, CA 91302 +511 712 3990
MIP	Abila	Sistema de Finanzas \$13,000	Call Sales: 800-811-0961 Main Office Phone: 800-647-3863 Main Office Location: 10800 Pecan Park Blvd., Suite 400, Austin, Texas 78750
Kronnos	Kronnos	Sistema de Asistencia	100 Grand Boulevard Paseos PMB 275 San Juan, PR 00926
ADP	ADP	Sistema de Nómina	Michael Schneider 973-974-5678 michael.schneider@adp.com Steve Cross 973-974-5744 steven.r.cross@adp.com
Destiny	Follet Destiny	Sistema de catalogación de Biblioteca	Carretera núm. 1, Km 34.1, Reparto Industrial Cartagena, Caguas, Puerto Rico 00725 Mailing address: PO Box 6840, Caguas, PR 00726
Google Apps	Google	Correos electrónicos	https://support.google.com/accounts?hl=en#topic=3382296

Actualmente el servicio de “Web Server” se ofrece a través de un server dedicado en la nube con la compañía Hostmonster quien mantiene la página de Internet de la Escuela (www.eap.edu). Asimismo, se utiliza Google Apps para los correos electrónicos de toda la comunidad universitaria. La cuenta de cada usuario está vinculada a un Drive virtual donde se realiza el resguardo de datos automático. Estos servicios aun cuando residen en un servidor externo, son administrados por la OSI y el Centro de Diseño. La compañía procura el mantenimiento del equipo y el resguardo de los datos.

De igual forma, el sistema de catalogación Destiny, utilizado por el Centro de Recursos para el Aprendizaje fue integrado al servicio en la nube de la compañía Camera Mundi. A través del Internet se acceden todos los servicios y se mantiene la continuidad del mismo.

XIII. Red de comunicaciones

La Oficina de Sistemas de Información, ubicada en el Edificio Antiguo Manicomio tiene bajo su supervisión y custodia los equipos que componen la red de comunicación de la EAPD. Incluye dos switches de telefonía, de 24 puertos, marca Extreme Networks con número serial: 0720G-00615, tres switches marca Cisco, modelo SG200-26, con números de propiedad EAPD-4632,4633 y 4634.

En el Antiguo Hospital de la Concepción tenemos cuatro “wiring closets” (Biblioteca, Área de Estudios Generales, Laboratorio de Computadoras y Decanato de Asuntos Estudiantiles) los cuales se conectan entre sí mediante un "backbone" de fibra óptica.

XIV. Contraseñas

Cada empleado se le asigna en el “Active Directory” una contraseña que tiene que cambiar cuando ingresa por primera vez a su computadora. Además, cada 45 días el sistema le solicita cambiar la misma para propósitos de seguridad.

XV. Clasificación del equipo y los datos

El equipo más importante en la Escuela de Artes Plásticas y Diseño de Puerto Rico, en términos de tecnología, son los servidores. Todo este equipo está físicamente localizado en la OSI, donde se han implantado varias medidas de control y seguridad para reducir la probabilidad de daños al mismo. El servidor de control de dominio (primario y secundario) es el único que permanece en la Oficina de Sistemas de Información luego de haber migrado todas las demás aplicaciones a servidores virtuales. Todas estas aplicaciones pueden ser accedidas en caso de desastre desde cualquier lugar que tenga servicio de Internet para mantener la continuidad de los servicios.

A través de ambos edificios se encuentran equipos de comunicación “switches” que crean la red de telecomunicaciones de la EAPD. A continuación, se muestra la tabla de estos.

Tabla V: Inventario de switches en la red

Núm. Propiedad	Mac Address	Marca	Modelo	Datos Adicionales
FTX0904D13N	8002343505B0	Cisco	2800	Oficina de Sistemas. Router
EAP-4633	58:35:d9:10:1e:68	Cisco	SG 200-26	Oficina de Sistemas. Conecta la Administración
EAP-4632	58:35:d9:10:1e:82	Cisco	SG 200-26	Oficina de Sistemas. Conecta la Administración
EAP-4634	58:35:d9:0f:e:10	Cisco	SG 200-26	Oficina de Sistemas. Conecta la Administración

0720G-00615		Extreme Networks	Summit x250e-24p	Oficina de Sistemas. Cuadro Telefónico.
0731G-00739		Extreme Networks	Summit x250e-24p	Oficina de Sistemas. Cuadro Telefónico.
EAP-2918	00146C0b029a	Netgear	FSM7352S	Anfiteatro Antiguo Manicomio.
EAP-2608	000a04a199b8	3com	3300	Salón de Pintura. Antigua Biblioteca.
EAP-4635	58:35:d9:10:1e:b6	Cisco	SG 200-26	Laboratorio. Conecta el pasillo y Salón HLC5
9T4NC21	00:30:ab:23:fd:3c	Dell	PowerConnect 3048	Laboratorio. Conecta Salones HLC6 y HLC7
HS4NC21		Dell	PowerConnect 3048	Laboratorio. Se utiliza para el proceso de matrícula
GS4NC21	0030AB23FC EB	Dell	PowerConnect 3048	Laboratorio. Conecta Salon HLC2 y HLC3
FHK0610W1E6	0009430832C0	CISCO	CATALYST 2950	Laboratorio. Conecta Salón HLC4 y el CITA
FHK0610X1JK	000943083840	CISCO	CATALYST 2950	Laboratorio. Conecta los servers
1TTHY21	000BDF82DDA	Dell	PowerConnect3348	Salón 324. Conecta el Switch de la antena con el Principal de sistemas
37VHY21	000BDBF8211A	Dell	PowerConnect3348	Biblioteca. Conecta con la antena
8T4NC21	0030AB23FE1F	Dell	PowerConnect3048	Oficina Decana. Conecta las Oficinas del Decanato

XVI Procedimientos de resguardo y recuperación

Los programas de producción mencionados anteriormente se encuentran en la nube que es manejada por la compañía que los desarrolló. Ellos se encargan de mantener un resguardo de los datos. Además utilizamos la cuenta de correo electrónico backup@eap.edu para subir todos los documentos relacionados a licencias y resguardos necesarios. La Oficial Principal de Informática y los técnicos de la OSI tienen acceso a este correo para realizar los resguardos del Active Directory. Cada usuario mantiene sus documentos en la computadora y se ha programado para que sincronice con su cuenta de correo electrónico al Google Drive. El mismo tiene capacidad ilimitada.

XVII. Medidas preventivas

La OSI tiene implementadas algunas medidas preventivas (controles generales) para reducir la probabilidad de interrupciones en las operaciones por diversas causas y para evitar el uso indebido de los recursos. Entre estas medidas se encuentran las siguientes:

1. División de labores a nivel de la estructura organizacional de OSI

2. Unidades independientes de aire acondicionado
3. Sistema de corriente ininterrumpida ("UPS")
4. Contraseñas para cada usuario (su cambio es forzado cada cuarenta y cinco días por el sistema operativo)
5. Usuarios son autorizados por la alta gerencia.
6. Sistema de protección Windows Defender
7. Almacenamiento de archivos en Google Drive
8. 2 Sistemas de "Firewall" Fortinet 100D y 50 E
9. Lista de contraseñas ("passwords") importantes en la cuenta backup@eap.edu

XVIII. Actualización

El presente documento debe ser actualizado cada vez que surjan cambios tecnológicos significativos en la EAPD e informar a la alta gerencia sobre los mismos.

Anejo I

Reporte de Incidente de Seguridad de la Información